



FEDERAL REGISTER

Vol. 89

Thursday,

No. 66

April 4, 2024

Pages 23497–23906

OFFICE OF THE FEDERAL REGISTER



The **FEDERAL REGISTER** (ISSN 0097-6326) is published daily, Monday through Friday, except official holidays, by the Office of the Federal Register, National Archives and Records Administration, under the Federal Register Act (44 U.S.C. Ch. 15) and the regulations of the Administrative Committee of the Federal Register (1 CFR Ch. I). The Superintendent of Documents, U.S. Government Publishing Office, is the exclusive distributor of the official edition. Periodicals postage is paid at Washington, DC.

The **FEDERAL REGISTER** provides a uniform system for making available to the public regulations and legal notices issued by Federal agencies. These include Presidential proclamations and Executive Orders, Federal agency documents having general applicability and legal effect, documents required to be published by act of Congress, and other Federal agency documents of public interest.

Documents are on file for public inspection in the Office of the Federal Register the day before they are published, unless the issuing agency requests earlier filing. For a list of documents currently on file for public inspection, see www.federalregister.gov.

The seal of the National Archives and Records Administration authenticates the **Federal Register** as the official serial publication established under the Federal Register Act. Under 44 U.S.C. 1507, the contents of the **Federal Register** shall be judicially noticed.

The **Federal Register** is published in paper and on 24x microfiche. It is also available online at no charge at www.govinfo.gov, a service of the U.S. Government Publishing Office.

The online edition of the **Federal Register** is issued under the authority of the Administrative Committee of the Federal Register as the official legal equivalent of the paper and microfiche editions (44 U.S.C. 4101 and 1 CFR 5.10). It is updated by 6:00 a.m. each day the **Federal Register** is published and includes both text and graphics from Volume 1, 1 (March 14, 1936) forward. For more information, contact the GPO Customer Contact Center, U.S. Government Publishing Office. Phone 202-512-1800 or 866-512-1800 (toll free). E-mail, gpocusthelp.com.

The annual subscription price for the **Federal Register** paper edition is \$860 plus postage, or \$929, for a combined **Federal Register**, **Federal Register** Index and List of CFR Sections Affected (LSA) subscription; the microfiche edition of the **Federal Register** including the **Federal Register** Index and LSA is \$330, plus postage. Six month subscriptions are available for one-half the annual rate. The prevailing postal rates will be applied to orders according to the delivery method requested. The price of a single copy of the daily **Federal Register**, including postage, is based on the number of pages: \$11 for an issue containing less than 200 pages; \$22 for an issue containing 200 to 400 pages; and \$33 for an issue containing more than 400 pages. Single issues of the microfiche edition may be purchased for \$3 per copy, including postage. Remit check or money order, made payable to the Superintendent of Documents, or charge to your GPO Deposit Account, VISA, MasterCard, American Express, or Discover. Mail to: U.S. Government Publishing Office—New Orders, P.O. Box 979050, St. Louis, MO 63197-9000; or call toll free 1-866-512-1800, DC area 202-512-1800; or go to the U.S. Government Online Bookstore site, see bookstore.gpo.gov.

There are no restrictions on the republication of material appearing in the **Federal Register**.

How To Cite This Publication: Use the volume number and the page number. Example: 89 FR 12345.

Postmaster: Send address changes to the Superintendent of Documents, Federal Register, U.S. Government Publishing Office, Washington, DC 20402, along with the entire mailing label from the last issue received.

SUBSCRIPTIONS AND COPIES

PUBLIC

Subscriptions:

Paper or fiche 202-09512-1800
Assistance with public subscriptions 202-512-1806

General online information 202-512-1530; 1-888-293-6498

Single copies/back copies:

Paper or fiche 202-512-1800
Assistance with public single copies 1-866-512-1800
(Toll-Free)

FEDERAL AGENCIES

Subscriptions:

Assistance with Federal agency subscriptions:

Email FRSubscriptions@nara.gov
Phone 202-741-6000

The Federal Register Printing Savings Act of 2017 (Pub. L. 115-120) placed restrictions on distribution of official printed copies of the daily **Federal Register** to members of Congress and Federal offices. Under this Act, the Director of the Government Publishing Office may not provide printed copies of the daily **Federal Register** unless a Member or other Federal office requests a specific issue or a subscription to the print edition. For more information on how to subscribe use the following website link: <https://www.gpo.gov/frsubs>.



Contents

Federal Register

Vol. 89, No. 66

Thursday, April 4, 2024

Agriculture Department

See Animal and Plant Health Inspection Service

See Food and Nutrition Service

See Food Safety and Inspection Service

See Forest Service

See Rural Business-Cooperative Service

Animal and Plant Health Inspection Service

RULES

Domestic Quarantine:

Quarantined Areas and Regulated Articles; Technical Amendment, 23500–23501

NOTICES

Imports:

Rosemary and Tarragon from Ethiopia, Pest Risk Analyses, 23537

Centers for Medicare & Medicaid Services

PROPOSED RULES

Medicare Program:

Fiscal Year 2025 Hospice Wage Index and Payment Rate, Hospice Conditions of Participation, and Hospice Quality Reporting Program Requirements, 23778–23838

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals, 23598–23599

Civil Rights Commission

NOTICES

Hearings, Meetings, Proceedings, etc.:

Tennessee Advisory Committee, 23560

Coast Guard

RULES

Safety Zone:

Kokosing ROV Survey Operation, Straits of Mackinac, MI, 23512–23514

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals, 23602–23604

Hearings, Meetings, Proceedings, etc.:

National Maritime Security Advisory Committee, 23601–23602

Commerce Department

See Industry and Security Bureau

See International Trade Administration

See National Oceanic and Atmospheric Administration

Drug Enforcement Administration

NOTICES

Importer, Manufacturer or Bulk Manufacturer of Controlled Substances; Application, Registration, etc.:

Benuvia Operations, LLC, 23612

Lonza Tampa, LLC, 23612

Patheon Pharmaceuticals Inc., 23611–23612

Sterling Wisconsin, LLC, 23611

Education Department

RULES

Augustus F. Hawkins Centers of Excellence Program, 23514–23518

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals:

Build America, Buy America Act Data Collection, 23592–23593

Evaluation of Transition Supports for Youth with Disabilities, 23573

Reaffirmation Agreement, 23565

Applications for New Awards:

Augustus F. Hawkins Centers of Excellence Program, 23565–23573

Teacher Quality Partnership Grant Program, 23573–23592

Employee Benefits Security Administration

NOTICES

Exemption:

Certain Prohibited Transaction Restrictions; Northern Trust Corp. (Together with its Current and Future Affiliates, Northern Trust or the Applicant); Technical Correction, 23612–23614

Energy Department

See Federal Energy Regulatory Commission

Environmental Protection Agency

RULES

Air Quality State Implementation Plans; Approvals and Promulgations:

Arizona; Maricopa County Air Quality Department, 23521–23523

Partial Denial of Petitions for Reconsideration: Federal Good Neighbor Plan for the 2015 Ozone National Ambient Air Quality Standards, 23526–23527

Pennsylvania; Allegheny County Open Burning Revision and Addition of Mon Valley Air Pollution Episode Requirements, 23523–23526

National Emission Standards for Hazardous Air Pollutants:

Ethylene Production, Miscellaneous Organic Chemical Manufacturing, Organic Liquids Distribution (Non-Gasoline), and Petroleum Refineries Reconsideration, 23840–23873

Federal Aviation Administration

RULES

Airspace Designations and Reporting Points:

San Juan Luis Munoz Marin International Airport, PR, 23510–23512

Special Conditions:

Airbus Model A321neo XLR Airplane; Electronic Flight-Control System: Lateral-Directional and Longitudinal Stability, and Low-Energy Awareness, 23507–23510

Jet Aviation AG, The Boeing Co. Model 737–8 Series Airplane; Dynamic Test Requirements for Single Occupant Oblique Seats With or Without Airbags and/or 3-Point Restraints, 23504–23507

PROPOSED RULES

Airspace Designations and Reporting Points:

Eastern United States, 23532–23534

Airworthiness Directives:

Embraer S.A. (Type Certificate Previously Held by Yabora Industria Aeronautica S.A.; Embraer S.A.) Airplanes, 23529–23532

Federal Communications Commission**RULES**

Facilitating Shared Use in the 3100–3550 MHz Band;
Correction, 23527–23528

Federal Energy Regulatory Commission**NOTICES**

Combined Filings, 23593–23596
Environmental Assessments; Availability, etc.:
Georgia Power Co., 23594–23595
Seattle City Light, 23596
Environmental Site Review:
Consolidated Hydro New York, LLC, 23597–23598

Federal Motor Carrier Safety Administration**NOTICES**

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:
Apprenticeship Pilot Program, 23617–23618

Federal Transit Administration**NOTICES**

Guidance:
Rural Areas Formula Grant Programs Guidance Proposed
Circular, 23618–23621

Fish and Wildlife Service**PROPOSED RULES**

Endangered and Threatened Species:
Status with Section 4(d) Rule for the Northwestern Pond
Turtle and Southwestern Pond Turtle, 23534

Food and Drug Administration**NOTICES**

Guidance:
New Dietary Ingredient Notification Master Files for
Dietary Supplements, 23599–23600

Food and Nutrition Service**NOTICES**

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:
Assessment of Administrative Costs of Electronic Healthy
Incentives Projects, 23545–23550
Evaluating the Interview Requirement for Supplemental
Nutrition Assistance Program Certification Study,
23539–23545

Food Safety and Inspection Service**NOTICES**

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:
Voluntary Recalls of Meat, Poultry, and Egg Products,
23537–23539

Foreign Assets Control Office**NOTICES**

Sanctions Action, 23628–23636

Forest Service**NOTICES**

Newspapers Used for Publication of Legal Notices by the
Alaska Region, 23550
Newspapers Used for Publication of Legal Notices by the
Pacific Northwest Region, Oregon, Washington, and
Parts of California, 23550–23551

Health and Human Services Department

See Centers for Medicare & Medicaid Services

See Food and Drug Administration

See National Institutes of Health

Homeland Security Department

See Coast Guard

See U.S. Customs and Border Protection

RULES

Petitions for Rulemaking, Amendment, or Repeal; Technical
Amendment, 23499–23500
Procedures for Debarring Vessels from Entering U.S. Ports,
23501–23504

PROPOSED RULES

Cyber Incident Reporting for Critical Infrastructure Act,
23644–23776

Indian Affairs Bureau**NOTICES**

Rate Adjustments for Indian Irrigation Projects; Correction,
23606

Industry and Security Bureau**RULES**

Implementation of Additional Export Controls:
Certain Advanced Computing Items; Supercomputer and
Semiconductor End Use; Updates and Corrections;
and Export Controls on Semiconductor
Manufacturing Items; Corrections and Clarifications,
23876–23905

Interior Department

See Fish and Wildlife Service

See Indian Affairs Bureau

See Land Management Bureau

NOTICES

Agency Information Collection Activities; Proposals,
Submissions, and Approvals:
Programmatic Clearance for Customer Satisfaction
Surveys, 23607–23608
Watercraft Inspection and Decontamination Regional
Data-Sharing for Trailered Boats, 23606–23607

International Trade Administration**NOTICES**

Antidumping or Countervailing Duty Investigations, Orders,
or Reviews:
Forged Steel Fittings from the Republic of Korea, 23560–
23562

International Trade Commission**NOTICES**

Investigations; Determinations, Modifications, and Rulings,
etc.:
Melamine from Germany, India, Japan, Netherlands,
Qatar, and Trinidad and Tobago, 23610–23611
Rubber Bands from China and Thailand, 23610

Justice Department

See Drug Enforcement Administration

Labor Department

See Employee Benefits Security Administration

Land Management Bureau**NOTICES**

Alaska Native Claims Selection, 23609–23610
Hearings, Meetings, Proceedings, etc.:
Central California Resource Advisory Council, 23608–
23609

Maritime Administration**NOTICES**

Coastwise Endorsement Eligibility Determination for a Foreign-Built Vessel:
 Dream (Motor), 23624–23625
 Ichthys (Motor), 23625–23626
 Kirin (Sail), 23621–23622
 RMM Job (Motor), 23623–23624
 Under Offer (Motor), 23622–23623

National Institutes of Health**NOTICES**

Hearings, Meetings, Proceedings, etc.:
 National Institute of Biomedical Imaging and Bioengineering, 23600–23601
 National Institute of Diabetes and Digestive and Kidney Diseases, 23601

National Oceanic and Atmospheric Administration**PROPOSED RULES**

Fisheries of the Exclusive Economic Zone off Alaska:
 Amendment 113 to the Fishery Management Plan for the Groundfish of the Gulf of Alaska; Central Gulf of Alaska Rockfish Program Adjustments, 23535–23536

NOTICES

Hearings, Meetings, Proceedings, etc.:
 Caribbean Fishery Management Council, 23562–23563
 North Pacific Fishery Management Council, 23564
 Pacific Fishery Management Council, 23563–23564
 South Atlantic Fishery Management Council, 23564–23565

Postal Regulatory Commission**NOTICES**

New Postal Products, 23614–23615

Postal Service**NOTICES**

Product Change:
 Priority Mail and Parcel Select Negotiated Service Agreement, 23615
 Priority Mail and USPS Ground Advantage Negotiated Service Agreement, 23615–23616
 Priority Mail Express Negotiated Service Agreement, 23615
 Priority Mail Express, Priority Mail and USPS Ground Advantage Negotiated Service Agreement, 23615

Presidential Documents**PROCLAMATIONS**

Special Observances:
 World Autism Awareness Day (Proc. 10725), 23497–23498

Rural Business-Cooperative Service**NOTICES**

Funding Opportunity:
 Rural Cooperative Development Grants for Fiscal Year 2024, 23551–23560

Small Business Administration**NOTICES**

Disaster or Emergency Declaration and Related Determination:
 Indiana, 23616–23617
 Maryland, 23616

Transportation Department

See Federal Aviation Administration

See Federal Motor Carrier Safety Administration
 See Federal Transit Administration
 See Maritime Administration

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals, 23626–23628

Treasury Department

See Foreign Assets Control Office

NOTICES

Interest Rate Paid:
 Cash Deposited to Secure U.S. Immigration and Customs Enforcement Immigration Bonds, 23636–23637

U.S. Customs and Border Protection**NOTICES**

Quarterly Interest Rates Used in Calculating Interest on Overdue Accounts and Refunds of Customs Duties, 23604–23605

U.S.-China Economic and Security Review Commission**NOTICES**

Hearings, Meetings, Proceedings, etc., 23637

Veterans Affairs Department**RULES**

Instructions for Determining Eligibility for In Vitro Fertilization Benefit, 23518–23521

NOTICES

Agency Information Collection Activities; Proposals, Submissions, and Approvals:
 Homeless Providers Grant and Per Diem Program, 23637–23638
 Privacy Act; Systems of Records, 23638–23641

Separate Parts In This Issue**Part II**

Homeland Security Department, 23644–23776

Part III

Health and Human Services Department, Centers for Medicare & Medicaid Services, 23778–23838

Part IV

Environmental Protection Agency, 23840–23873

Part V

Commerce Department, Industry and Security Bureau, 23876–23905

Reader Aids

Consult the Reader Aids section at the end of this issue for phone numbers, online resources, finding aids, and notice of recently enacted public laws.

To subscribe to the Federal Register Table of Contents electronic mailing list, go to <https://public.govdelivery.com/accounts/USGPOOFR/subscriber/new>, enter your e-mail address, then follow the instructions to join, leave, or manage your subscription.

CFR PARTS AFFECTED IN THIS ISSUE

A cumulative list of the parts affected this month can be found in the Reader Aids section at the end of this issue.

3 CFR**Proclamations:**

10725.....23497

6 CFR

3.....23499

Proposed Rules:

226.....23644

7 CFR

301.....23500

8 CFR

258.....23501

14 CFR

25 (2 documents)23504,

23507

71.....23510

Proposed Rules:

39.....23529

71.....23532

15 CFR

732.....23876

734.....23876

736.....23876

740.....23876

742.....23876

744.....23876

746.....23876

748.....23876

758.....23876

770.....23876

772.....23876

774.....23876

33 CFR

165.....23512

34 CFR

Ch. VI.....23514

38 CFR

17.....23518

40 CFR

52 (3 documents)23521,

23523, 23526

63.....23840

75.....23526

78.....23526

97.....23526

42 CFR**Proposed Rules:**

418.....23778

47 CFR

2.....23527

50 CFR**Proposed Rules:**

17.....23534

679.....23535

Presidential Documents

Title 3—

Proclamation 10725 of April 1, 2024

The President

World Autism Awareness Day, 2024

By the President of the United States of America**A Proclamation**

America was founded on the idea that all people are created equal and deserve to be treated equally throughout their lives. Today, we champion the equal rights and dignity of the millions of Americans on the autism spectrum, and we celebrate the immense contributions of all neurodiverse people, whose perspectives and experiences make America a richer Nation.

Some 5.4 million American adults and 1 in 36 children have been diagnosed with autism. Their experiences with the condition vary widely, but their talents and potential are too often misunderstood or overlooked. Autistic people routinely face unnecessary obstacles to securing employment and health care and children face bullying and barriers to education. We can work to end these disparities and ensure they have an equal opportunity to reach their dreams by making sure that people with autism and those who support them have the resources and tools they need to communicate, grow, work, and achieve greater independence.

Early diagnosis can make a big difference, which is why my Administration is funding groundbreaking research to boost access to diagnoses and services that can help autistic people of all ages thrive. The Department of Education and the Department of Health and Human Services are also working to ensure that young children with disabilities, including autism, have access to high-quality, inclusive early childhood programs so that they can thrive as well as helping schools leverage Medicaid to deliver critical health care services. Further, my Administration released guidance on how schools can obtain, use, and support assistive technology devices that are essential to the success of some people with disabilities. Meanwhile, the Department of Education is helping public schools avoid discriminatory discipline for autistic students, whose needs can be misunderstood, while also working to get students with autism and their teachers the resources they need to thrive. We are working to boost understanding among community members who can help keep people with autism safe—I was proud to sign a reauthorization of Kevin and Avonte's Law, expanding training for first responders and caregivers.

My Administration is also making it easier for all Americans to get the health care they need. We protected and strengthened the Affordable Care Act and Medicaid, expanding health care coverage to millions of Americans. At the same time, we lowered health insurance premiums by \$800 per year for millions of Americans. Through the American Rescue Plan, we provided \$37 billion to make it easier for people with disabilities, including autism, to receive the services they need at home and stay active in their communities. My Budget requests another \$150 billion over the next decade to further expand and improve these life-changing services.

We owe everyone in this country a fair shot at the American Dream, so we are also working to increase job opportunities for autistic and other historically marginalized Americans who have been shut out for too long. My Administration is providing State and local governments, private companies, and nonprofits with Federal funding to hire more Americans with disabilities, including those with autism. I signed an Executive Order to

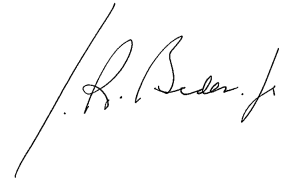
make the Federal workforce more inclusive, and I eliminated the unjust use of sub-minimum wages for people with disabilities by Federal contractors, working to ensure every American has equal protection under the law.

Globally, we are advancing disability rights as part of our work to promote democracy, prosperity, and inclusion. We are prioritizing disability rights in policy discussions with other nations, and we are working through the United States Agency for International Development and as co-chair of the Global Action on Disability Network to stand for the dignity and equal rights of people with disabilities worldwide.

Diversity in all its forms is one of America's greatest strengths. Today, we recommit to making the promise of America real for every American on the autism spectrum, upholding our most basic values of decency, fairness, and respect.

NOW, THEREFORE, I, JOSEPH R. BIDEN JR., President of the United States of America, by virtue of the authority vested in me by the Constitution and the laws of the United States, do hereby proclaim April 2, 2024, as World Autism Awareness Day. I call upon all Americans to learn more about autism to improve early diagnosis, to learn more about the experiences of autistic people from autistic people, and to build more welcoming and inclusive communities to support people with autism.

IN WITNESS WHEREOF, I have hereunto set my hand this first day of April, in the year of our Lord two thousand twenty-four, and of the Independence of the United States of America the two hundred and forty-eighth.



Rules and Regulations

Federal Register

Vol. 89, No. 66

Thursday, April 4, 2024

This section of the FEDERAL REGISTER contains regulatory documents having general applicability and legal effect, most of which are keyed to and codified in the Code of Federal Regulations, which is published under 50 titles pursuant to 44 U.S.C. 1510.

The Code of Federal Regulations is sold by the Superintendent of Documents.

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 3

Petitions for Rulemaking, Amendment, or Repeal; Technical Amendment

AGENCY: Office of the Secretary, Department of Homeland Security (DHS).

ACTION: Final rule; technical amendment.

SUMMARY: This final rule amends the affected regulation by correcting a cross-reference error and updating the mailing address interested persons should use when submitting a petition for rulemaking to the Transportation Security Administration (TSA). This action does not create or change any substantive requirement or right.

DATES: This rule is effective April 4, 2024.

FOR FURTHER INFORMATION CONTACT: David F. Graham, Attorney-Advisor, U.S. Department of Homeland Security, Office of the General Counsel, 245 Murray Lane SW, Mail Stop 0485, Washington, DC 20528-0485, telephone (202) 814-0416.

SUPPLEMENTARY INFORMATION:

I. Discussion of the Rule

The Administrative Procedure Act (APA) requires that each agency give interested persons the right to petition the agency for the issuance, amendment, or repeal of a rule.¹ Such a petition is known as a “rulemaking petition.” On November 28, 2016, the DHS published a final rule describing its procedures for receiving and responding to rulemaking petitions.² Among other provisions, the 2016 final rule identified the mailing address for rulemaking petitions

directed towards the Transportation Security Administration as Transportation Security Administration, Office of the Chief Counsel, TSA-2, Attn: Regulations and Security Standards Division, 601 South 12th Street, Arlington, VA 20598-6002. The 2016 final rule also advised that rulemaking petitions directed towards the Federal Emergency Management Agency (FEMA) were governed by 44 CFR 1.18.

The mailing address for the TSA Office of Chief Counsel has changed from 601 South 12th Street, Arlington, VA 20598-6002, to 6595 Springfield Center Drive, Springfield, VA 20598-6002. This action amends 6 CFR 3.5(b)(2) to reflect the TSA’s current and correct mailing address for receiving rulemaking petitions.

In addition, the cross-reference to 44 CFR 1.18 is no longer current. Specifically, rulemaking petitions directed towards FEMA are now governed by 44 CFR 1.8. This action amends 6 CFR 3.3(b)(2) to reflect the correct citation.

II. Regulatory Analyses

DHS considered numerous statutes and executive orders related to rulemaking when developing this technical amendment. Below are summarized analyses based on those statutes and executive orders.

A. Administrative Procedure Act

DHS has determined that this rule is exempt from notice-and-comment rulemaking requirements under 5 U.S.C. 553(b)(A) and 5 U.S.C. 553(b)(B). The amendments in this rule provide non-substantive technical, organizational, and conforming updates to a rule that itself constitutes a “rule of agency organization, procedure, or practice” not subject to the Administrative Procedure Act’s (APA) notice and comment requirements under 5 U.S.C. 553(b)(A). In addition, these amendments are technical or editorial non-substantive changes, which are intended to update and correct two provisions within the CFR. These amendments are necessary to ensure the accuracy and clarity of the CFR. Neither of the amendments included in this action will have a substantive impact on the public, nor will they alter any substantive regulatory requirements. Accordingly, DHS finds for good cause that this final rule is exempt from public

notice-and-comment rulemaking procedures under 5 U.S.C. 553(b)(B) because such procedures are unnecessary.

Because this rule is procedural in nature, DHS finds that the 30-day delayed effective date requirement for substantive rules does not apply, *see* 5 U.S.C. 553(d). In addition, because affected parties will not need time to adjust to the revisions made through this action, DHS finds that even if a 30-day delayed effective date requirement did apply to this action, good cause exists to make this technical amendment effective upon publication in the **Federal Register** under 5 U.S.C. 553(d)(3).

B. Regulatory Flexibility Act and Executive Order 12866

Because DHS has determined that this final rule is exempt from notice and comment rulemaking requirements, the provisions of the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*) do not apply to this action. Furthermore, this final rule does not meet the criteria for a “significant regulatory action” as specified in Executive Order 12866.

C. Paperwork Reduction Act

There is no new or amended collection of information required by this action. Therefore, the provisions of the Paperwork Reduction Act of 1995 are inapplicable.

D. National Environmental Policy Act (NEPA)

DHS reviews proposed actions to determine whether the National Environmental Policy Act (NEPA) applies to them and, if so, what degree of analysis is required. DHS Directive 023-01 Rev. 01 (Directive) and Instruction Manual 023-01-001-01 Rev. 01 (Instruction Manual) establish the procedures that DHS and its components use to comply with NEPA and the Council on Environmental Quality (CEQ) regulations for implementing NEPA, 40 CFR parts 1500 through 1508.

The CEQ regulations allow Federal agencies to establish, with CEQ review and concurrence, categories of actions (“categorical exclusions”) which experience has shown do not individually or cumulatively have a significant effect on the human environment and, therefore, do not require an Environmental Assessment

¹ 5 U.S.C. 553(e).

² 81 FR 85401; *see also* 81 FR 47285 (July 21, 2016) (interim final rule).

(EA) or Environmental Impact Statement (EIS). 40 CFR 1507.3(b)(2)(ii), 1508.4. For an action to be categorically excluded, it must satisfy each of the following three conditions: (1) the entire action clearly fits within one or more of the categorical exclusions; (2) the action is not a piece of a larger action; and (3) no extraordinary circumstances exist that create the potential for a significant environmental effect. Instruction Manual section V.B(2)(a)–(c).

This final rule is a technical amendment that provides non-substantive technical and organizational updates. Therefore, it clearly fits within categorical exclusion A3(a) “Promulgation of rules . . . of a strictly administrative or procedural nature.” Instruction Manual, Appendix A, Table 1. Furthermore, this final rule is not part of a larger action and presents no extraordinary circumstances creating the potential for significant environmental impacts. Therefore, the amendment is categorically excluded from further NEPA review.

E. Federalism

Under Executive Order 13132 (Federalism), agencies must consider whether a rule has federalism implications. DHS has determined that this technical amendment does not have federalism implications because it does not create a substantial direct effect on States, on the relationship between the National Government and States, or the distribution of power and responsibilities among the various levels of government.

F. Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act of 1995, 2 U.S.C. 1531–38, requires agencies to consider whether a rule will result in the expenditure of \$100,000,000 or more (adjusted annually for inflation) in any one year by State, local, and Tribal governments, in the aggregate, or by the private sector. This technical amendment will not result in such an expenditure.

G. The Congressional Review Act

Before a rule can take effect, 5 U.S.C. 801, the Congressional Review Act requires agencies to submit the rule and a report indicating whether it is a major rule to Congress and the Comptroller General. Under 5 U.S.C. 804(3)(C), rules of agency organization, procedure, or practice that do not substantially affect the rights or obligations of non-agency parties are not considered to be a rule for the purposes of the Congressional Review Act. This citation correction, as well as the updated mailing address constitute a rule of agency organization,

procedure, or practice that will have no substantive effect on the public. Thus, DHS is not required to submit this technical amendment to Congress and the Comptroller General under the Congressional Review Act.

List of Subjects in 6 CFR Part 3

Administrative practice and procedure, Petitions for rulemaking.

For the reasons stated in the preamble, the Department of Homeland Security amends 6 CFR part 3 as follows:

PART 3—PETITIONS FOR RULEMAKING

- 1. The authority citation for part 3 continues to read as follows:

Authority: 5 U.S.C. 301, 553(e); 6 U.S.C. 112.

§ 3.3 [Amended]

- 2. In § 3.3(b)(2), remove the text “44 CFR 1.18” and add, in its place, the text “44 CFR 1.8”.

§ 3.5 [Amended]

- 3. In § 3.5(b)(2), remove the text “601 South 12th Street, Arlington, VA 20598–6002” and add, in its place, the text “6595 Springfield Center Drive, Springfield, VA 20598–6002”.

Alejandro N. Mayorkas,

Secretary, U.S. Department of Homeland Security.

[FR Doc. 2024–07034 Filed 4–3–24; 8:45 am]

BILLING CODE 9111–9B–P

DEPARTMENT OF AGRICULTURE

Animal and Plant Health Inspection Service

7 CFR Part 301

[Docket No. APHIS–2019–0035]

RIN 0579–AE62

Domestic Quarantine: Quarantined Areas and Regulated Articles; Technical Amendment

AGENCY: Animal and Plant Health Inspection Service, Department of Agriculture (USDA).

ACTION: Final rule; technical amendment.

SUMMARY: In a final rule published in the *Federal Register* on December 29, 2022, and effective on January 30, 2023, we amended the regulations governing domestic quarantines for various plant pests by removing lists of quarantined areas and regulated articles from the regulations in order to maintain these

lists on web pages maintained by the Agency. However, in the regulations governing black stem rust, we incorrectly stated that the web page listing articles determined to be rust-resistant only listed species and varieties of the genus *Berberis*, rather than species and varieties of the genera *Berberis*, *Mahoberberis*, and *Mahonia*. Therefore, we are amending the paragraph to correct the omission.

DATES: Effective April 4, 2024.

FOR FURTHER INFORMATION CONTACT: Ms. Lynn Evans-Goldner, National Policy Manager, Office of the Deputy Administrator, PPQ, APHIS, 4700 River Road, Unit 137, Riverdale, MD 20737; (301) 851–2286; lynn.evans-goldner@usda.gov.

SUPPLEMENTARY INFORMATION: In a final rule¹ that was published in the *Federal Register* on December 29, 2022 (87 FR 80002), and effective on January 30, 2023, we amended the regulations governing domestic quarantines for various plant pests by removing lists of quarantined areas and regulated articles from the regulations in order to maintain these lists on web pages maintained by the Agency. One of the affected subparts was “Subpart D—Black Stem Rust” (7 CFR 301.38 through 301.38–8). Section 301.38–2(b) correctly states that species and varieties of the genera *Berberis*, *Mahoberberis*, and *Mahonia* are regulated articles. However, in § 301.38–2(a), which provides the web page where regulated articles are listed, we inadvertently excluded the genera *Mahoberberis* and *Mahonia*, incorrectly implying that the list on the web page is limited to species of *Berberis*. This document corrects that error.

List of Subjects in 7 CFR Part 301

Agricultural commodities, Plant diseases and pests, Quarantine, Reporting and recordkeeping requirements, Transportation.

Accordingly, we amend 7 CFR part 301 as follows:

PART 301—DOMESTIC QUARANTINE NOTICES

- 1. The authority citation for part 301 continues to read as follows:

Authority: 7 U.S.C. 7701–7772 and 7781–7786; 7 CFR 2.22, 2.80, and 371.3.

Section 301.75–15 issued under Sec. 204, Title II, Public Law 106–113, 113 Stat. 1501A–293; sections 301.75–15 and 301.75–16 issued under Sec. 203, Title II, Public Law 106–224, 114 Stat. 400 (7 U.S.C. 1421 note).

¹To view the final rule and supporting documents, go to: <https://www.regulations.gov/document/APHIS-2019-0035-0002>.

§ 301.38–2 [Amended]

■ 2. Amend § 301.38–2, in paragraph (a), by adding the words “, *Mahoberberis*, and *Mahonia*” after the word “*Berberis*” in the first sentence.

Done in Washington, DC, this 28th day of March 2024.

Donna Lalli,

Acting Administrator, Animal and Plant Health Inspection Service.

[FR Doc. 2024–07038 Filed 4–3–24; 8:45 am]

BILLING CODE 3410–34–P

DEPARTMENT OF HOMELAND SECURITY**8 CFR Part 258**

[Docket No. USCBP–2022–0016]

RIN 1651–AB20

[CBP Dec. 24–07]

Procedures for Debarring Vessels From Entering U.S. Ports

AGENCY: U.S. Customs and Border Protection, Department of Homeland Security.

ACTION: Final rule.

SUMMARY: This final rule amends Department of Homeland Security (DHS) regulations by adding procedures regarding DHS’s authority to debar from entering U.S. ports vessels owned or chartered by an entity found to be in violation of certain laws and regulations relating to the performance of longshore work by nonimmigrant crew members. The new procedures govern how U.S. Customs and Border Protection (CBP) provides notice to a vessel owner or operator of a debarment and how the owner or operator may request mitigation. The new procedures will ensure that the vessel debarment process is consistent, fair, and transparent.

DATES: This final rule is effective on May 6, 2024.

FOR FURTHER INFORMATION CONTACT: Lisa Santana Fox, Director, Fines, Penalties and Forfeitures Division, Office of Field Operations, U.S. Customs and Border Protection, at 202–344–2730 or Lisa.K.SanatanaFox@cbp.dhs.gov.

SUPPLEMENTARY INFORMATION:**I. Background and Legal Authority**

Section 258 of the Immigration and Nationality Act of 1952 (INA) (Pub. L. 82–414, 66 Stat. 163), as amended, prohibits alien crew members (classified as nonimmigrants under section 101(a)(15)(D) of the INA, 8 U.S.C. 1101(a)(15)(D)) from entering the United

States to perform longshore work,¹ subject to certain statutory exceptions. See INA 258, 8 U.S.C. 1288; see also INA 101(a)(15)(D) and 214(f), 8 U.S.C. 1101(a)(15)(D) and 1184(f). The INA authorizes the Department of Homeland Security (DHS) and the Secretary of Labor to investigate violations of, and enforce the INA provisions relating to, the performance of longshore work by nonimmigrant crew members. See INA 251(d) and 258(c)(4)(E)(i), 8 U.S.C. 1281(d) and 1288(c)(4)(E)(i); see also 20 CFR 655.600 and 655.605. The Secretary of Labor will notify the Secretary of Homeland Security (Secretary) if the Secretary of Labor determines that a violation has occurred. See INA 258(c)(4)(E)(i), 8 U.S.C. 1288(c)(4)(E)(i). The INA then directs the Secretary to debar any vessel or vessels owned or chartered by the violating entity from entering U.S. ports for a period not to exceed one year. See INA 258(c)(4)(E)(i), 8 U.S.C. 1288(c)(4)(E)(i); 8 CFR 258.1(a)(2). The Secretary has delegated to the Commissioner of U.S. Customs and Border Protection (CBP) the authority to enforce and administer INA provisions relating to longshore work, including the authority to debar a vessel. See DHS Delegation No. 7010.3(B)(11) (Revision No. 03.1).

DHS regulations implementing the longshore work requirements are set forth in title 8 of the Code of Federal Regulations (CFR) parts 251 and 258. See 8 CFR 251 and 258. However, DHS regulations do not include procedures for CBP to follow when debarring a vessel, nor do they state how a vessel owner or operator may request mitigation of a debarment. In 2022, DHS published a notice of proposed rulemaking (NPRM) to add procedures for how CBP would notify an entity of a debarment and how a vessel owner or operator, or its authorized representative, may request mitigation of the debarment. See 87 FR 21582 (April 12, 2022). The NPRM proposed procedures to generally codify the steps CBP took in 2009 and 2010, the only times CBP has imposed debarments.

¹ Longshore work is defined as any activity in the United States or in U.S. coastal waters relating to the loading or unloading of cargo, the operation of cargo-related equipment (whether or not integral to the vessel), and the handling of mooring lines on the dock when the vessel is made fast or let go. See INA 258(b)(1), 8 U.S.C. 1288(b)(1). Longshore work does not include the loading or unloading of certain cargo including oil and hazardous substances and materials for which the Secretary of Transportation has prescribed regulations governing cargo handling or storage; the manning of vessels and the duties, qualifications, and training of the officers and crew of vessels carrying such cargo; and, the reduction or elimination of discharge during ballasting, tank cleaning, and handling of such cargo. See INA 258(b)(2), 8 U.S.C. 1288(b)(2).

The purpose of the NPRM was to establish consistent, fair, and transparent debarment procedures for both CBP and the entity subject to the debarment.

The NPRM provided for a 60-day comment period, which closed on June 13, 2022. No comments were received. DHS is adopting the NPRM as final without change.

II. Procedures for Debarring Vessels From Entering U.S. Ports

This final rule adds 8 CFR 258.4, which specifies the procedures that CBP will take prior to issuing a debarment and describe how a vessel owner or operator, or its authorized representative, may request mitigation of the debarment. These new procedures are described below.

A. Definitions

Paragraph (a) of section 258.4 sets forth definitions for the following terms for purposes of CBP’s debarment proceedings: good cause, mitigation, and mitigation meeting. Good cause, for purposes of extending the deadline for filing an answer, includes technical difficulties or natural disasters that affect the violating entity’s ability to receive, process, or transmit relevant information or data; or other instances in which CBP, in its discretion, determines an undue hardship on the violating entity warrants an extension of the deadline for filing an answer. See 8 CFR 258.4(a).

Mitigation in a debarment proceeding means determining the length of the debarment, the ports covered by the debarment, and the vessels subject to the debarment. It does not include revocation of the requirement to debar. See 8 CFR 258.4(a).

CBP notes that a violating entity may mitigate its length of debarment by showing that a specific period of debarment would have a negative impact on the U.S. economy and/or U.S. citizens/consumers. Examples of this include showing that a specific period of business activity (*i.e.*, fishing season) will be negatively impacted if a vessel were debarred, or that a vessel will be transporting produce or a type of perishable consumer good to the United States within a specific time frame for which debarment would be detrimental.

Mitigation meeting is a personal appearance before a designated CBP official in which representatives of the violating entity can provide information and explain why CBP should mitigate the debarment. See 8 CFR 258.4(a).

B. Notice of Intent To Debar

Paragraph (b) of section 258.4 sets forth the procedures pertaining to the issuance of a notice of intent to debar and specifies the information to be included in such notice. After receiving notice from the Secretary of Labor that an entity has violated the relevant statutes or regulations, CBP will serve a notice of intent to debar on the entity subject to the notice of violation. *See* 8 CFR 258.4(b)(1). Service will be by a method that demonstrates receipt, such as certified mail with return receipt or express courier delivery, by the entity identified in the notice of violation received from the Secretary of Labor. The date of service is the date of receipt. *See* 8 CFR 258.4(b)(3).

The notice of intent to debar will include specific information, including: the proposed period of debarment, not to exceed one year; the ports covered by the proposed debarment; a brief explanation of the reasons for the proposed debarment; the statutory and regulatory authority for the proposed debarment; a statement that the entity subject to the debarment may file an answer and request a mitigation meeting; the procedures for filing an answer and requesting a mitigation meeting, including the date by which the answer must be received and the address to which it may be submitted; and, a statement that in the absence of a timely filed answer, the proposed debarment will become final 30 days after service of the notice of intent to debar. *See* 8 CFR 258.4(b)(2)(i) through (vii).

C. Answer and Request for Mitigation Meeting

Paragraph (c) of section 258.4 describes how an entity should file an answer with CBP and how to request mitigation and a mitigation meeting. Any entity upon which the notice of intent to debar has been served, or its authorized representative, may file with CBP an answer that indicates the specific reasons why the proposed debarment should be mitigated and whether a mitigation meeting is requested. CBP must receive the answer within 30 days from the date of service of the notice of intent to debar. *See* 8 CFR 258.4(c)(1). As explained previously, the date of service of the notice of intent to debar is the date the entity received the notice. *See* 8 CFR 258.4(b)(3).

CBP, in its discretion, may extend the deadline for filing an answer up to an additional 30 days upon a showing of good cause as defined in 8 CFR 258.4(a). Upon receipt of a request to extend the

deadline, CBP will respond within five business days by certified mail or express courier. *See* 8 CFR 258.4(c)(2)(iv).

The answer must be dated, typewritten or legibly written, signed under oath, and include the address at which the entity, or its authorized representative, desires to receive further communication. CBP may require that the answer and any supporting documentation be in English or be accompanied by an English translation, certified by a competent translator. *See* 8 CFR 258.4(c)(2)(i).

In addition to an answer, any entity responding to a notice of intent to debar must submit documentary evidence in support of any request for mitigation and may file a brief in support of any arguments made. The entity may also present evidence in support of any request for mitigation at a mitigation meeting. *See* 8 CFR 258.4(c)(2)(ii). A mitigation meeting will be conducted if the entity subject to the proposed debarment requests one in accordance with the requirements of this rule, or if directed at any time by CBP. *See* 8 CFR 258.4(c)(2)(iii).

D. Disposition of Case

Paragraph (d) of section 258.4 describes how CBP will determine a final order of debarment for each case. The proposed debarment specified in the notice of intent to debar will automatically become a final order of debarment 30 days after service of the notice of intent to debar if no answer is timely filed or if the answer admits the allegations and does not request mitigation or a mitigation meeting. *See* 8 CFR 258.4(d)(1). If CBP grants a good cause extension to the deadline for filing an answer, but no answer is timely filed, the proposed debarment will automatically become a final order of debarment when the time for filing an answer expires. *See* 8 CFR 258.4(c)(2)(iv) and (d)(1).

If an entity timely files an answer that requests mitigation or a mitigation meeting, CBP will determine a final debarment and will issue to the entity a final order of debarment in writing.² CBP will also send notice, by certified mail or express courier, to all interested parties, including the relevant U.S. ports of entry, that the entity subject to the debarment is debarred and stating the terms of the debarment. No appeal from

²The information received from the Secretary of Labor, evidence or arguments timely presented by the entity subject to the debarment, and any other relevant factors that CBP considers in its determination of the debarment will be disclosed in its final determination of debarment to the violating entity.

a final order of debarment will be available. *See* 8 CFR 258.4(d)(2)–(3).

E. Debarment

Paragraph (e) of section 8 CFR 258.4 describes the information CBP will consider when determining a proposed debarment or a final debarment. It specifies that CBP, in determining a proposed and a final debarment, will consider the information received from the Secretary of Labor, any evidence or arguments timely presented by the entity subject to the debarment, and other relevant factors. *See* 8 CFR 258.4(e)(1). Other relevant factors include, but are not limited to: the entity's previous history of violations of any provision of the INA; the number of U.S. workers adversely affected by the violation; the gravity of the violation; the entity's efforts to comply in good faith with regulatory and statutory requirements governing performance of longshore work by nonimmigrant crew members; the entity's remedial efforts and commitment to future compliance; the extent of the entity's cooperation with the investigation; and, the entity's financial gain/loss due to the violation. CBP will also consider the potential financial loss, injury, or adverse effect to other parties, including U.S. workers, likely to result from the debarment. *See* 8 CFR 258.4(e)(2).

F. Notice of Completion of Debarment

Paragraph (f) of section 258.4 states that upon completion of any debarment, CBP will send notice, by certified mail or express courier, to all interested parties, including the entity subject to the debarment and the relevant U.S. ports of entry, that the entity subject to the debarment has completed the debarment and is once again permitted to enter U.S. ports.

G. Record

Paragraph (g) of section 258.4 states that CBP will keep a record of the debarment proceedings, which includes, but is not limited to, the materials exchanged between CBP and the parties. The provision further states that CBP will retain the records in accordance with CBP's Records Retention Schedule and the Freedom of Information Act. Currently, this means CBP will retain records for five years, after which the records will be sent to the National Archives.

III. Statutory and Regulatory Analysis

A. Executive Orders 12866 and 13563

Executive Orders 12866 (Regulatory Planning and Review), as amended by Executive Order 14094 (Modernizing Regulatory Review), and 13563

(Improving Regulation and Regulatory Review), direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, reducing costs, harmonizing rules, and promoting flexibility.

The Office of Management and Budget (OMB) has not designated this rule a significant regulatory action under section 3(f) of Executive Order 12866, as amended by Executive Order 14094. Accordingly, OMB has not reviewed this regulation.

Pursuant to section 258 of the INA, CBP has the authority to debar vessels. See INA 258, 8 U.S.C. 1288. This final rule does not create that requirement. Rather, this final rule would codify and clarify existing practice, with some exceptions, that CBP follows in carrying out that requirement. Accordingly, even without this rule, CBP still has the authority to debar vessels. This rule is being promulgated to avoid confusion and to have, in writing, a clear and consistent process for the debarment of vessels.

CBP has debarred vessels in only two instances in its recorded history, in 2009 and 2010. As described above, the final rule will generally codify the procedures CBP followed when debarring vessels in 2009 and 2010, with changes only to the type of mail service CBP uses to serve notices of intent to debar. The process for debarring vessels that CBP has followed is not changing as a result of this rule. Therefore, this rule has no economic impact on violating entities.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*), as amended by the Small Business Regulatory Enforcement and Fairness Act of 1996, requires agencies to assess the impact of regulations on small entities. A small entity may be a small business (defined as any independently owned and operated business not dominant in its field that qualifies as a small business per the Small Business Act); or a small not-for-profit organization; or a small governmental jurisdiction (locality with fewer than 50,000 people).

As explained above, pursuant to section 258 of the INA, CBP is required to debar vessels in certain situations. This rule does not create such a requirement. Instead, this final rule

would codify and clarify the existing procedures, with some exceptions, that CBP follows in carrying out that requirement. These procedures are seldom used, as CBP has debarred vessels in only two instances, once in 2009 and a second instance occurring in 2010. Furthermore, CBP is generally adopting existing practices, and accordingly, costs to violating entities will not change as a result of this final rule. CBP thus certifies that this final rule will not have a significant economic impact on a substantial number of small entities.

C. Paperwork Reduction Act

The Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. 3507(d)) requires that CBP consider the impact of paperwork and other information collection burdens imposed on the public. An agency may not conduct, and a person is not required to respond to, a collection of information unless the collection of information displays a valid control number assigned by the Office of Management and Budget. There is no information collection associated with this final rule, so the provisions of the PRA do not apply.³

D. Congressional Review Act

The Congressional Review Act (5 U.S.C. 801 *et seq.*), as amended, generally provides that before a major rule may take effect, the agency promulgating the rule must submit a rule report, which includes a copy of the rule, to each House of the Congress and to the Comptroller General of the United States. Under the Congressional Review Act, a major rule is one that is likely to result in an annual effect on the U.S. economy of \$100,000,000 or more. See 5 U.S.C. 804(2). This final rule is not a “major rule” as defined by the Congressional Review Act.

E. Unfunded Mandates Reform Act

Title II of the Unfunded Mandates Reform Act of 1995, enacted as Public Law 104–4 on March 22, 1995, requires each Federal agency, to the extent permitted by law, to prepare a written assessment of the effects of any Federal mandate in a proposed or final agency rule that may result in the expenditure by state, local, and tribal governments, in the aggregate, or by the private sector, of \$100 million or more (adjusted annually for inflation) in any one year. See 2 U.S.C. 1532(a). This rule will not result in the expenditure by state, local, and tribal governments, in the aggregate, or by the private sector, of \$100 million

³ The required Department of Labor attestations are covered by OMB Control Number 1205–0309.

or more in any one year. Therefore, no actions were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

IV. Signing Authority

This regulation is being issued in accordance with 19 CFR 0.2(a) pertaining to the Secretary of Homeland Security’s authority (or that of his delegate) to approve regulations that are not related to customs revenue functions.

List of Subjects in 8 CFR Part 258

Aliens, Longshore and harbor workers, Reporting and recordkeeping requirements, Seamen.

For the reasons stated in the preamble, DHS amends part 258 of title 8 of the Code of Federal Regulations as follows:

PART 258—LIMITATIONS ON PERFORMANCE OF LONGSHORE WORK BY ALIEN CREWMEN

■ 1. The authority citation for part 258 continues to read as follows:

Authority: 8 U.S.C. 1101, 1103, 1281; 8 CFR part 2.

■ 2. Add new § 258.4 to read as follows:

§ 258.4 Debarment of vessels.

(a) *Definitions.* The following definitions apply throughout this section:

Good cause, for purposes of extending the deadline for filing an answer, includes: technical difficulties or natural disasters that affect the violating entity’s ability to receive, process, or transmit relevant information or data; or other instances in which CBP, in its discretion, determines that an undue hardship on the violating entity warrants an extension of the deadline for filing an answer.

Mitigation in a debarment proceeding means determining the length of the debarment, the ports covered by the debarment, and the vessels subject to the debarment. It does not include revocation of the requirement to debar.

Mitigation meeting is a personal appearance before a designated CBP official in which representatives of the violating entity can provide information and explain why CBP should mitigate the debarment.

(b) *Notice of intent to debar.*

(1) *Issuance of notice.* Upon receipt of a notice of violation from the Secretary of Labor pursuant to section 258 of the Immigration and Nationality Act (8 U.S.C. 1288(c)(4)(E)(i)), CBP will serve a notice of intent to debar on the entity subject to the notice of violation, as

provided in paragraph (b)(3) of this section.

(2) *Contents of notice.* The notice of intent to debar will include the following:

(i) The proposed period of debarment, not to exceed one year;

(ii) The ports covered by the proposed debarment;

(iii) A brief explanation of the reasons for the proposed debarment;

(iv) The statutory and regulatory authority for the proposed debarment;

(v) A statement that the entity subject to the debarment may file an answer and request a mitigation meeting pursuant to paragraph (c) of this section;

(vi) The procedures for filing an answer and requesting a mitigation meeting, including the date by which the answer must be received and the address to which it may be submitted; and

(vii) A statement that in the absence of a timely filed answer, the proposed debarment will become final 30 days after service of the notice of intent to debar.

(3) *Service.* The notice of intent to debar will be served by a method that demonstrates receipt, such as certified mail with return receipt or express courier delivery, by the entity identified in the notice of violation received from the Secretary of Labor. The date of service is the date of receipt.

(c) *Answer; request for mitigation meeting.*

(1) *General.* Any entity upon which the notice has been served, or its authorized representative, may file with CBP an answer that indicates the specific reasons why the proposed debarment should be mitigated and whether a mitigation meeting is requested. CBP must receive the answer within 30 days from the date of service of the notice of intent to debar.

(2) *Procedures.*

(i) *Form.* The answer must be dated, typewritten or legibly written, signed under oath, and include the address at which the entity or its authorized representative desires to receive further communications. CBP may require that the answer and any supporting documentation be in English or be accompanied by an English translation certified by a competent translator.

(ii) *Supporting documentation required.* In addition to an answer, any entity responding to a notice of intent to debar must submit documentary evidence in support of any request for mitigation and may file a brief in support of any arguments made. The entity may present evidence in support of any request for mitigation at a mitigation meeting.

(iii) *Mitigation meeting.* A mitigation meeting will be conducted if requested by the entity subject to the proposed debarment in accordance with the requirements of this section, or if directed at any time by CBP.

(iv) *Good cause extension.* CBP, in its discretion, may extend the deadline for filing an answer up to an additional 30 days from the original receipt of CBP's notice upon a showing of good cause. Upon receipt of a request to extend the deadline for filing an answer, CBP will respond to the request for an extension within 5 business days by certified mail or express courier.

(d) *Disposition of case.*

(1) *No response filed or allegations not contested.* If no answer is timely filed or the answer admits the allegations in the notice of intent to debar and does not request mitigation or a mitigation meeting, the proposed debarment specified in the notice of intent to debar automatically will become a final order of debarment 30 days after service of the notice of intent to debar. If CBP grants a good cause extension pursuant to paragraph (c)(2)(iv) of this section, and no answer is timely filed, the proposed debarment automatically will become a final order of debarment when the time for filing an answer expires.

(2) *Answer filed; mitigation meeting requested.* If an answer is timely filed that requests mitigation and/or a mitigation meeting, CBP will determine a final debarment in accordance with paragraph (e) of this section.

(3) *Unavailability of appeal.* The final order of debarment is not subject to appeal.

(4) *Notice of final order of debarment.*

(i) CBP will issue to the entity subject to the debarment a final order of debarment in writing.

(ii) CBP will send notice, by certified mail or express courier, to all interested parties, including the relevant U.S. ports of entry, that the entity subject to the debarment is debarred and stating the terms of the debarment.

(e) *Debarment.*

(1) *Generally.* In determining a proposed debarment and a final debarment, CBP will consider the information received from the Secretary of Labor, any evidence or arguments timely presented by the entity subject to the debarment, and any other relevant factors.

(2) *Other relevant factors.* Other relevant factors include, but are not limited to, the following:

(i) The previous history of violations of any provision of the INA by the entity subject to the debarment;

(ii) The number of U.S. workers adversely affected by the violation;

(iii) The gravity of the violation;

(iv) The efforts made by the entity subject to the debarment to comply in good faith with the regulatory and statutory requirements governing performance of longshore work by nonimmigrant crewmen;

(v) The remedial efforts by the entity subject to the debarment;

(vi) The commitment to future compliance by the entity subject to the debarment;

(vii) The extent of cooperation with the investigation by the entity subject to the debarment;

(viii) The extent of financial gain/loss to the entity subject to the debarment due to the violation; and

(ix) The potential financial loss, injury, or adverse effect to other parties, including U.S. workers, likely to result from the debarment.

(f) *Notice of completion of debarment.*

Upon completion of any debarment, CBP will send notice, by certified mail or express courier, to all interested parties, including the entity subject to the debarment, and the relevant U.S. ports of entry, that the entity subject to the debarment has completed the debarment and is once again permitted to enter U.S. ports.

(g) *Record.* CBP will keep a record of the debarment proceedings which includes, but is not limited to, the materials exchanged between CBP and the parties. Records will be retained in accordance with CBP's Records Retention Schedule and the Freedom of Information Act.

Alejandro N. Mayorkas,

Secretary, U.S. Department of Homeland Security.

[FR Doc. 2024-07169 Filed 4-3-24; 8:45 am]

BILLING CODE 9111-14-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 25

[Docket No. FAA-2024-0448; Special Conditions No. 25-859-SC]

Special Conditions: Jet Aviation AG, The Boeing Company Model 737-8 Series Airplane; Dynamic Test Requirements for Single Occupant Oblique Seats With or Without Airbags and/or 3-Point Restraints

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final special conditions; request for comments.

SUMMARY: These special conditions are issued for The Boeing Company (Boeing) Model 737–8 series airplane. This airplane, as modified by Jet Aviation AG (Jet Aviation), will have a novel or unusual design feature when compared to the state of technology envisioned in the airworthiness standards for transport-category airplanes. This design feature is oblique (side-facing) single-occupant seats equipped with airbag devices or 3-point restraints. The applicable airworthiness regulations do not contain adequate or appropriate safety standards for this design feature. These special conditions contain the additional safety standards that the Administrator considers necessary to establish a level of safety equivalent to that established by the existing airworthiness standards.

DATES: This action is effective on Jet Aviation on April 4, 2024. Send comments on or before May 20, 2024.

ADDRESSES: Send comments identified by Docket No. FAA–2024–0448 using any of the following methods:

- *Federal eRegulations Portal:* Go to <https://www.regulations.gov/> and follow the online instructions for sending your comments electronically.

- *Mail:* Send comments to Docket Operations, M–30, U.S. Department of Transportation (DOT), 1200 New Jersey Avenue SE, Room W12–140, West Building Ground Floor, Washington, DC 20590–0001.

- *Hand Delivery or Courier:* Take comments to Docket Operations in Room W12–140 of the West Building Ground Floor at 1200 New Jersey Avenue SE, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

- *Fax:* Fax comments to Docket Operations at 202–493–2251.

- *Docket:* Background documents or comments received may be read at <https://www.regulations.gov/> at any time. Follow the online instructions for accessing the docket or go to Docket Operations in Room W12–140 of the West Building Ground Floor at 1200 New Jersey Avenue SE, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

FOR FURTHER INFORMATION CONTACT: John Shelden, Cabin Safety Section, AIR–624, Technical Policy Branch, Policy and Standards Division, Aircraft Certification Service, Federal Aviation Administration, 2200 South 216th Street, Des Moines, Washington 98198; telephone and fax 206–231–3214; email John.Shelden@faa.gov.

SUPPLEMENTARY INFORMATION: The substance of these special conditions has been published in the **Federal**

Register for public comment in several prior instances with no substantive comments received. Therefore, the FAA finds, pursuant to 14 CFR 11.38(b), that new comments are unlikely, and notice and comment prior to this publication are unnecessary.

Privacy

Except for Confidential Business Information (CBI) as described in the following paragraph, and other information as described in title 14, Code of Federal Regulations (14 CFR) 11.35, the FAA will post all comments received without change to www.regulations.gov, including any personal information you provide. The FAA will also post a report summarizing each substantive verbal contact received about these special conditions.

Confidential Business Information

Confidential Business Information (CBI) is commercial or financial information that is both customarily and actually treated as private by its owner. Under the Freedom of Information Act (FOIA) (5 U.S.C. 552), CBI is exempt from public disclosure. If your comments responsive to these special conditions contain commercial or financial information that is customarily treated as private, that you actually treat as private, and that is relevant or responsive to these special conditions, it is important that you clearly designate the submitted comments as CBI. Please mark each page of your submission containing CBI as “PROPIN.” The FAA will treat such marked submissions as confidential under the FOIA, and the indicated comments will not be placed in the public docket of these special conditions. Send submissions containing CBI to the individual listed in the **FOR FURTHER INFORMATION CONTACT** section above. Comments the FAA receives, which are not specifically designated as CBI, will be placed in the public docket for these proposed special conditions.

Comments Invited

The FAA invites interested people to take part in this rulemaking by sending written comments, data, or views. The most helpful comments reference a specific portion of the special conditions, explain the reason for any recommended change, and include supporting data.

The FAA will consider all comments received by the closing date for comments, and will consider comments filed late if it is possible to do so without incurring delay. The FAA may

change these special conditions based on the comments received.

Background

On December 19, 2022, Jet Aviation applied for a supplemental type certificate for the installation of oblique (side-facing) passenger seats with or without airbag devices or 3-point restraints in the Boeing Model 737–8 series airplanes. The Boeing Model 737–8 series airplane is a twin-engine, transport category airplane with a maximum takeoff weight of approximately 182,200 lbs. The airplane, as modified by Jet Aviation, will have a maximum seating capacity of 32.

Type Certification Basis

Under the provisions of title 14, Code of Federal Regulations (14 CFR) 21.101, Jet Aviation must show that the Model 737–8 series airplanes, as changed, continue to meet the applicable provisions of the regulations listed in Type Certificate No. A16WE or the applicable regulations in effect on the date of application for the change, except for earlier amendments as agreed upon by the FAA.

If the Administrator finds that the applicable airworthiness regulations (*i.e.*, 14 CFR part 25) do not contain adequate or appropriate safety standards for the Boeing Model 737–8 series airplane because of a novel or unusual design feature, special conditions are prescribed under the provisions of § 21.16.

Special conditions are initially applicable to the model for which they are issued. Should the type certificate for that model be amended later to include any other model that incorporates the same novel or unusual design feature, or should any other model already included on the same type certificate be modified to incorporate the same novel or unusual design feature, the special conditions would also apply to the other model under § 21.101.

In addition to the applicable airworthiness regulations and special conditions, the Boeing Model 737–8 series airplane must comply with the exhaust-emission requirements of 14 CFR part 34, and the noise-certification requirements of 14 CFR part 36.

The FAA issues special conditions, as defined in 14 CFR 11.19, in accordance with § 11.38, and they become part of the type certification basis under § 21.101.

Novel or Unusual Design Features

The Boeing Model 737–8 series airplane, as modified by Jet Aviation,

will incorporate a seating configuration that is novel or unusual due to the installation of oblique (side-facing) passenger seats and surrounding furniture that introduces occupant alignment and loading concerns. These oblique seats may be installed at an angle of 18 to 45 degrees to the aircraft centerline and may include a 3-point restraint system and/or airbags, for occupant restraint and injury protection.

Discussion

Title 14, Code of Federal Regulations (14 CFR) 25.785(d) requires that each occupant of a seat that makes more than an 18 degree angle with the vertical plane containing the airplane centerline must be protected from head injury by a safety belt and an energy absorbing rest that will support the arms, shoulders, head, and spine, or by a safety belt and shoulder harness that will prevent the head from contacting any injurious object.

The proposed Boeing Model 737-8 airplane seat installation is novel in that the current requirements do not adequately address protection of the occupant's neck and spine for seating configurations that are positioned at angles greater than 18 degrees up to and including 45 degrees from the airplane centerline. The installation of passenger seats at angles of 18 to 45 degrees to the airplane centerline is unique due to the seat/occupant interface with the surrounding furniture that introduces occupant alignment/loading concerns with or without the installation of a 3-point or airbag restraint system, or both.

In order to provide a level of safety that is equivalent to that afforded to occupants of forward and aft facing seating, additional airworthiness standards, in the form of new special conditions, are necessary.

The FAA has been conducting and sponsoring research on appropriate injury criteria for oblique (side-facing) seat installations. To reflect current research findings, the FAA issued Policy Statement PS-AIR-25-27. FAA-sponsored research has found that an unrestrained flailing of the upper torso, even when the pelvis and torso are nearly aligned, can produce serious spinal and torso injuries. At lower impact severities, even with significant misalignment between the torso and pelvis, these injuries did not occur. Tests with an FAA H-III anthropomorphic test dummy (ATD) have identified a level of lumbar spinal tension corresponding to the no-injury impact severity. This level of tension is included as a limit in the special conditions. The spine tension limit selected is conservative with respect to

other aviation injury criteria since it corresponds to a no-injury loading condition.

As noted in the special conditions, because each airbag restraint system is essentially a single use device, there is the potential that it could deploy under crash conditions that are not sufficiently severe as to require head injury protection from the airbag restraint system. Since an actual crash is frequently composed of a series of impacts before the airplane comes to rest, this could render the airbag restraint system useless if a larger impact follows the initial impact. This situation does not exist with energy absorbing pads or upper torso restraints, which tend to provide protection according to the severity of the impact. Therefore, the installation of the airbag restraint system should be such that the airbag restraint system will provide protection when it is required and will not expend its protection when it is not needed.

Because these airbag restraint systems may or may not activate during various crash conditions, the injury criteria listed in these special conditions and in § 25.562 must be met in an event that is slightly below the activation level of the airbag restraint system. If an airbag restraint system is included with the oblique seats, the system must meet the requirements in one of the airbag (inflatable restraint) special conditions applicable to the Boeing Model 737 series airplanes. These special conditions supplement part 25 and, more specifically, supplement §§ 25.562 and 25.785.

These special conditions contain the additional safety standards that the Administrator considers necessary to establish a level of safety equivalent to that established by the existing airworthiness standards.

Applicability

As discussed above, these special conditions are applicable to the Boeing Model 737-8 series airplane modified by Jet Aviation. Should Jet Aviation apply at a later date for a supplemental type certificate to modify any other model included on Type Certificate No. A16WE to incorporate the same novel or unusual design feature, or should Jet Aviation apply for a change to the supplemental type certificate to include another model to incorporate the same novel or unusual design feature, these special conditions would apply to that model as well.

Conclusion

This action affects only a certain novel or unusual design feature on one

model series of airplanes. It is not a rule of general applicability and affects only the applicant who applied to the FAA for approval of these features on the airplane.

List of Subjects in 14 CFR Part 25

Aircraft, Aviation safety, Reporting and recordkeeping requirements.

Authority Citation

The authority citation for these special conditions is as follows:

Authority: 49 U.S.C. 106(f), 106(g), 40113, 44701, 44702, and 44704.

The Special Conditions

■ Accordingly, pursuant to the authority delegated to me by the Administrator, the following special conditions are issued as part of the type certification basis for The Boeing Company Model 737-8 series airplanes modified by Jet Aviation AG.

In addition to the requirements of § 25.562, passenger seats installed at an angle between 18 degrees and 45 degrees from the aircraft centerline must meet the following:

1. Head Injury Criteria (HIC)

Compliance with § 25.562(c)(5) is required, except that, if the anthropomorphic test dummy (ATD) has no apparent contact with the seat/structure but has contact with an airbag, a HIC unlimited score in excess of 1000 is acceptable, provided the HIC15 score (calculated in accordance with 49 CFR 571.208) for that contact is less than 700.

2. Body-to-Wall/Furnishing Contact

If a seat is installed aft of a structure (e.g., interior wall or furnishings) that does not provide a homogenous contact surface for the expected range of occupants and yaw angles, then additional analysis and tests may be required to demonstrate that the injury criteria are met for the area that an occupant could contact. For example, if different yaw angles could result in different airbag device performance, then additional analysis or separate tests may be necessary to evaluate performance.

3. Neck Injury Criteria

The seating system must protect the occupant from experiencing serious neck injury. The assessment of neck injury must be conducted with the airbag device activated, unless there is reason to also consider that the neck-injury potential would be higher for impacts below the airbag-device deployment threshold.

a. The N_{ij} (calculated in accordance with 49 CFR 571.208) must be below 1.0, where $N_{ij} = F_z/F_{zc} + M_y/M_{yc}$, and N_{ij} critical values are:

- i. $F_{zc} = 1530$ lbs. for tension
- ii. $F_{zc} = 1385$ lbs. for compression
- iii. $M_{yc} = 229$ lb-ft in flexion
- iv. $M_{yc} = 100$ lb-ft in extension

b. In addition, peak F_z must be below 937 lbs. in tension and 899 lbs. in compression.

c. Rotation of the head about its vertical axis relative to the torso is limited to 105 degrees in either direction from forward facing.

d. The neck must not impact any surface that would produce concentrated loading on the neck.

4. Spine and Torso Injury Criteria

a. The lumbar spine tension (F_z) cannot exceed 1200 lbs.

b. Significant concentrated loading on the occupant's spine, in the area between the pelvis and shoulders during impact, including rebound, is not acceptable. During this type of contact, the interval for any rearward (X direction) acceleration exceeding 20g must be less than 3 milliseconds as measured by the thoracic instrumentation specified in 49 CFR part 572, subpart E filtered in accordance with SAE International (SAE) recommended practice J211/1, "Instrumentation for Impact Test—Part 1—Electronic Instrumentation."

c. The occupant must not interact with the armrest or other seat components in any manner significantly different than would be expected for a forward-facing seat installation.

5. Pelvis Criteria

Any part of the load-bearing portion of the bottom of the ATD pelvis must not translate beyond the edges of the seat bottom seat-cushion supporting structure.

6. Femur Criteria

Axial rotation of the upper leg (about the z-axis of the femur per SAE Recommended Practice J211/1) must be limited to 35 degrees from the nominal seated position. Evaluation during rebound does not need to be considered.

7. ATD and Test Conditions

Longitudinal tests conducted to measure the injury criteria above must be performed with the FAA Hybrid III ATD, as described in SAE 1999-01-1609, "A Lumbar Spine Modification to the Hybrid III ATD for Aircraft Seat Tests." The tests must be conducted with an undeformed floor, at the most-critical yaw cases for injury, and with

all lateral structural supports (*e.g.*, armrests or walls) installed.

Note: Jet Aviation AG must demonstrate that the installation of seats via plinths or pallets meets all applicable requirements. Compliance with the guidance contained in Policy Memorandum PS-ANM-100-2000-00123, "Guidance for Demonstrating Compliance with Seat Dynamic Testing for Plinths and Pallets," dated February 2, 2000, is acceptable to the FAA.

8. Inflatable Airbag Restraint Systems Special Conditions

If inflatable airbag restraint systems are installed, the airbag systems must meet the requirements in Special Conditions 25-386-SC, or other airbag system special conditions which are applicable to the Boeing Model 737 series airplanes.

Issued in Kansas City, Missouri, on March 22, 2024.

Patrick R. Mullen,

Manager, Technical Policy Branch, Policy and Standards Division, Aircraft Certification Service.

[FR Doc. 2024-06894 Filed 4-3-24; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 25

[Docket No. FAA-2021-1034; Special Conditions No. 25-857-SC]

Special Conditions: Airbus Model A321neo XLR Airplane; Electronic Flight-Control System: Lateral-Directional and Longitudinal Stability, and Low-Energy Awareness

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final special conditions.

SUMMARY: These special conditions are issued for the Airbus Model A321neo XLR airplane. This airplane will have a novel or unusual design feature when compared to the state of technology envisioned in the applicable airworthiness standards. This design feature is an electronic flight-control system (EFCS) associated with lateral-directional and longitudinal stability, and low-energy awareness. The applicable airworthiness regulations do not contain adequate or appropriate safety standards for this design feature. These special conditions contain the additional safety standards that the Administrator considers necessary to establish a level of safety equivalent to that established by the existing airworthiness standards.

DATES: Effective April 4, 2024.

FOR FURTHER INFORMATION CONTACT: Troy Brown, Performance and Environment Unit, AIR-621A, Technical Policy Branch, Policy and Standards Division, Aircraft Certification Service, Federal Aviation Administration, 1801 S Airport Rd., Wichita, KS 67209-2190; telephone and fax 405-666-1050; email troy.a.brown@faa.gov.

SUPPLEMENTARY INFORMATION:

Background

On September 16, 2019, Airbus applied for an amendment to Type Certificate No. A28NM to include the new Model A321neo XLR airplane. This airplane is a twin-engine, transport-category airplane, with seating for 244 passengers, and a maximum takeoff weight of 222,000 pounds.

Type Certification Basis

Under the provisions of 14 CFR 21.101, Airbus must show that the Model A321neo XLR airplane meets the applicable provisions of the regulations listed in Type Certificate No. A28NM, or the applicable regulations in effect on the date of application for the change, except for earlier amendments as agreed upon by the FAA.

If the Administrator finds that the applicable airworthiness regulations (*e.g.*, 14 CFR part 25) do not contain adequate or appropriate safety standards for the Airbus Model A321neo XLR airplane because of a novel or unusual design feature, special conditions are prescribed under the provisions of § 21.16.

Special conditions are initially applicable to the model for which they are issued. Should the type certificate for that model be amended later to include any other model that incorporates the same novel or unusual design feature, or should any other model already included on the same type certificate be modified to incorporate the same novel or unusual design feature, these special conditions would also apply to the other model under § 21.101.

In addition to the applicable airworthiness regulations and special conditions, the Airbus Model A321neo XLR airplane must comply with the fuel-vent and exhaust-emission requirements of 14 CFR part 34, and the noise-certification requirements of 14 CFR part 36.

The FAA issues special conditions, as defined in § 11.19, in accordance with § 11.38, and they become part of the type certification basis under § 21.101.

Novel or Unusual Design Feature

The Airbus Model A321neo XLR airplane will incorporate the following novel or unusual design feature:

An EFCS associated with lateral-directional and longitudinal stability, and low-energy awareness.

Proposed Special Conditions

The FAA issued Notice of Proposed Special Conditions No. FAA–2021–1034, which was published in the **Federal Register** on November 3, 2023 (88 FR 75517).

In that document, the FAA explained that the Airbus' proposed A321neo XLR includes an EFCS, and that the control laws of that system can result in neutral static lateral-directional stability and neutral static longitudinal stability, insufficient feedback to the flightcrew from the pitching moment, and insufficient awareness that the airplane is in a low-energy state. The FAA therefore proposed that the applicable airworthiness regulations are inadequate or inappropriate to address these issues and proposed special conditions to address them.

The FAA proposed that in the absence of positive lateral stability, the curve of lateral control-surface deflections against sideslip angle should be, in a conventional sense and reasonably in harmony with, rudder deflection during steady-heading sideslip maneuvers.

The FAA further proposed that because conventional relationships between stick forces and control-surface displacements do not apply to the "load-factor command" flight-control system on the Airbus Model A321neo XLR airplane, longitudinal stability characteristics should be evaluated by assessing the airplane's handling qualities during simulator and flight-test maneuvers appropriate to operation of the airplane. Additionally, under icing and non-icing conditions there may be a difference in full pedal deflection. This difference may result in changes to testing before reaching full pedal deflection, and these special conditions account for these differences.

The airplane must provide adequate awareness cues to the pilot of a low-energy (low-speed/low-thrust/low-height) state to ensure that the airplane retains sufficient energy to recover when flight-control laws provide neutral longitudinal stability significantly below the normal operating speeds. "Adequate awareness" means that information must be provided to alert the crew of unsafe operating conditions and to enable them to take appropriate corrective action. Testing of these awareness cues should occur by

simulator and flight test in the operational flight envelope for which certification is requested. Testing should include a sufficient number of tests to allow the level of energy awareness, and the effects of energy-management errors, to be assessed.

Discussion of Comments and Final Special Conditions

Airbus Commercial Aircraft (Airbus) and The Boeing Company (Boeing) submitted comments on the same provision of the proposed special conditions.

The Static Lateral-Directional Stability section of the proposed special conditions required the applicant to conduct, in icing conditions, steady heading sideslip maneuvers in several configurations. The proposed conditions would have required these sideslip maneuvers to be conducted "over the range of sideslip angles appropriate to the operation of the airplane, but not less than those obtained with one half of available rudder control input."

Airbus and Boeing each recommended that these maneuvers be conducted with full pedal deflection but recommended different approaches to implement that change.

Airbus requested that the FAA add a note stating that these maneuvers will be continued beyond the sideslip angles appropriate for normal operation of the airplane and demonstrate that full pedal travel can be safely applied. Airbus stated that deflecting the pedals as much as practicable in icing conditions would provide a better coverage of the intent of § 25.21(g) regarding § 25.177. Further, Airbus stated that the addition of this note would align FAA and EASA standards.

Boeing recommended that the FAA revise the special conditions to require Airbus to conduct these sideslips "up to the angle at which full rudder control is used or a rudder control force of 180 pounds is obtained." Boeing said this change would be consistent with the language of paragraph 4.15.2.3 of AC 25–25A, Performance and Handling Characteristics in Icing Conditions.

AC 25–25A provides an acceptable means of showing compliance with certain requirements of part 25 of 14 CFR related to airplane performance and handling characteristics in icing conditions. To address static lateral directional stability, the AC provides, as examples of an acceptable test program, that the applicant may conduct steady heading sideslips, in certain configurations, including "to full rudder authority, 180 pounds of rudder pedal force, or full lateral control authority." Paragraph 4.15.2.3.

The FAA agrees with the commenters that full-pedal deflection meets the intent of § 25.21(g) and aligns with guidance in the referenced AC. The FAA also agrees that this approach is harmonized with EASA's certification approach² to this issue. The FAA finds that it is unnecessary to revise the condition as suggested by Boeing, and that the language provided by Airbus, with minor revision by the FAA,³ is sufficient to address this issue.

These final special conditions correct minor discrepancies in the numbering of the proposed special conditions. Also, the proposed special conditions related to low energy awareness contained three instances of "should." The FAA has revised these to "must" in these final special conditions, for enforceability and for consistency with the expectations of the FAA and the applicant.

Other than these foregoing changes, these special conditions are adopted as proposed. The special conditions contain the additional safety standards that the Administrator considers necessary to establish a level of safety equivalent to that established by the existing airworthiness standards.

Applicability

As discussed above, these special conditions are applicable to the Airbus Model A321neo XLR airplane. Should Airbus apply at a later date for a change to the type certificate to include another model incorporating the same novel or unusual design feature, these special conditions would apply to that model as well.

Under standard practice, the effective date of final special conditions would be 30 days after the date of publication in the **Federal Register**. However, as the certification date for the Airbus Model A321neo XLR is imminent, the FAA finds that good cause exists to make these special conditions effective upon publication.

Conclusion

This action affects only certain novel or unusual design features on one model series of airplane. It is not a rule of general applicability.

² EASA Certification Review Item (CRI) B–06, "Flight in Icing Conditions", issue 2, April 11, 2013.

³ Under the U.S. regulatory system, notes are explanatory rather than mandatory. See, e.g., section 7.5 of the Document Drafting Handbook (Aug. 2018 Edition, Rev. 2.1, dated Oct. 2023). Therefore, in the final special conditions, the recommended language is no longer a "note," and the commenter's "will" is a "must."

List of Subjects in 14 CFR Part 25

Aircraft, Aviation safety, Reporting and recordkeeping requirements.

Authority Citation

The authority citation for these special conditions is as follows:

Authority: 49 U.S.C. 106(f), 106(g), 40113, 44701, 44702, 44704.

The Special Conditions

■ Accordingly, pursuant to the authority delegated to me by the Administrator, the following special conditions are issued as part of the type certification basis for the Airbus Model A321neo XLR airplane.

Static Lateral-Directional Stability

(a) In lieu of compliance with § 25.171, the airplane must have lateral and directional stability characteristics in accordance with § 25.177. In addition, both suitable stability and suitable control feel are required in any condition normally encountered in service.

(b) In lieu of compliance with § 25.177(c), the following requirement must be met for the configurations and speed specified in § 25.177(a):

(1) In straight, steady sideslips over the range of sideslip angles appropriate to the operation of the airplane, the directional control movements and forces must be substantially proportional to the angle of sideslip in a stable sense. The factor of proportionality must lie between limits found necessary for safe operation. During these straight, steady sideslips, necessary lateral control movements and forces must not be in the unstable sense with the exception of speeds above V_{mo}/M_{mo} per § 25.177(b)(2). The range of sideslip angles evaluated must include those sideslip angles resulting from the lesser of:

- (i) One-half of the available directional (pedal) control input; and
- (ii) A directional (pedal) control force of 180 pounds.

(c) In lieu of compliance with § 25.177(d), the following requirements must be met:

(1) In non-icing conditions, for sideslip angles greater than those prescribed by § 25.177(a), up to the angle at which full rudder control is used or a rudder control force of 180 pounds is obtained, the rudder control forces may not reverse, and increased rudder deflection must be needed for increased angles of sideslip. Compliance with this requirement must be shown using straight, steady sideslips, unless full lateral control input is achieved before reaching either full rudder

control input or a rudder control force of 180 pounds; a straight, steady sideslip need not be maintained after achieving full lateral control input. This requirement must be met at all approved landing gear and flap positions for the range of operating speeds and power conditions appropriate to each landing gear and flap position with all engines operating.

(2) In icing conditions, in the configurations listed below, trim the airplane at the specified speed and conduct steady heading sideslips over the range of sideslip angles appropriate to the operation of the airplane but not less than those obtained with one-half of available rudder control input.

(i) High lift devices retracted configuration: trim at best rate of climb speed but not less than minimum all engines operating climb speed defined for icing conditions.

(ii) Lowest lift take-off configuration: trim at the all-engines operating initial climb speed defined for icing conditions.

(iii) Landing configurations: trim at minimum landing speed defined for icing conditions.

The steady heading sideslip maneuver must be continued beyond sideslip angles appropriate for normal operation of the airplane to demonstrate full pedal can be safely applied unless justification for smaller input is provided (e.g., heavy buffet that would deter the pilot from further deflecting the pedals and would make investigations to full pedal a potential flight test safety concern, or pedal input required for normal operations significantly smaller than full pedal).

Longitudinal Stability

In lieu of compliance with the requirements of §§ 25.171, 25.173, and 25.175, the airplane must be shown to have longitudinal stability characteristics in accordance with the following conditions. In addition, both suitable stability and suitable control feel are required in any condition normally encountered in service, including the effects of atmospheric disturbance.

(a) Strong positive static longitudinal stability (1 pound per 6 knots applied through the sidestick) must be present which provides adequate awareness cues to the crew that the speed is above V_{mo}/M_{mo} or below the minimum speed for hands-free stabilized flight. Static longitudinal characteristics must be shown to be suitable based on the airplane handling qualities, including an evaluation of pilot workload and pilot compensation, for specific test procedures during the flight-test

evaluations. These characteristics must be shown for appropriate combinations of airplane configuration (i.e., flaps extended or retracted, gear deployed or stowed) and thrust for climb, cruise, approach, landing, and go-around.

(1) Release of the controller at speeds above V_{mo}/M_{mo} , or below the minimum speed for hands-free stabilized flight, must produce a prompt recovery towards normal operating speeds without resulting in a hazardous condition.

(2) The design must not allow a pilot to re-trim the controller forces resulting from this stability.

Low Energy Awareness

The airplane must provide adequate awareness cues to the pilot of a low-energy (low-speed/low-thrust/low-height) state to ensure that the airplane retains sufficient energy to recover when flight-control laws provide neutral longitudinal stability significantly below the normal operating speeds. This must be accomplished as follows:

(a) Adequate low speed/low thrust cues at low altitude should be provided by a strong positive static stability force gradient (1 pound per 6 knots applied through the sidestick), or

(b) The low energy awareness must be provided by an appropriate warning with the following characteristics. The low-energy awareness must:

- (1) Be unique, unambiguous, and unmistakable.
- (2) Be active at appropriate altitudes and in appropriate configurations (i.e., at low altitude, in the approach and landing configurations).
- (3) Be sufficiently timely to allow recovery to a stabilized flight condition inside the normal flight envelope while maintaining the desired flight path and without entering the flight controls angle-of-attack protection mode.
- (4) Not be triggered during normal operation, including operation in moderate turbulence for recommended maneuvers at recommended speeds.
- (5) Not be cancelable by the pilot other than by achieving a higher energy state.
- (6) Have an adequate hierarchy among the various warnings so that the pilot is not confused and led to take inappropriate recovery action if multiple warnings occur.

Global energy awareness and non-annoyance on low-energy cues must be evaluated by simulator and flight tests in the whole take-off and landing altitude range for which certification is requested. This includes all relevant combinations of weight, center-of-gravity position, configuration, airbrakes position, and available thrust, including

reduced and derated take-off thrust operations and engine-failure cases. The tests must assess the level of energy awareness, and the effects of energy-management errors.

Issued in Kansas City, Missouri, on March 28, 2024.

Patrick R. Mullen,

Manager, Technical Innovation Policy Branch, Policy and Innovation Division, Aircraft Certification Service.

[FR Doc. 2024-07139 Filed 4-3-24; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 71

[Docket No. FAA-2023-1906; **Airspace**
Docket No. 22-AWA-3]

RIN 2120-AA66

Amendment of Class C Airspace; San Juan Luis Munoz Marin International Airport, PR

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: This action modifies the San Juan Luis Munoz Marin International Airport, PR (SJU), Class C airspace by adding a cutout to the surface area near the Fernando Luis Ribas Dominicci Airport, PR (SIG). The FAA is taking this action to enhance safety and enable more efficient operations at SJU and SIG.

DATES: Effective date 0901 UTC, July 11, 2024. The Director of the Federal Register approves this incorporation by reference action under 1 CFR part 51, subject to the annual revision of FAA Order 7400.11 and publication of conforming amendments.

ADDRESSES: A copy of the Notice of Proposed Rulemaking (NPRM), all comments received, this final rule, and all background material may be viewed online at www.regulations.gov using the FAA Docket number. Electronic retrieval help and guidelines are available on the website. It is available 24 hours each day, 365 days each year.

FAA Order JO 7400.11H, Airspace Designations and Reporting Points, and subsequent amendments can be viewed online at www.faa.gov/air_traffic/publications/. You may also contact the Rules and Regulations Group, Office of Policy, Federal Aviation Administration, 800 Independence Avenue SW, Washington, DC 20591; telephone: (202) 267-8783.

FOR FURTHER INFORMATION CONTACT: Brian Vidis, Rules and Regulations Group, Office of Policy, Federal Aviation Administration, 800 Independence Avenue SW, Washington DC 20591; telephone: (202) 267-8783.

SUPPLEMENTARY INFORMATION:

Authority for This Rulemaking

The FAA's authority to issue rules regarding aviation safety is found in Title 49 of the United States Code. Subtitle I, Section 106 describes the authority of the FAA Administrator. Subtitle VII, Aviation Programs, describes in more detail the scope of the agency's authority. This rulemaking is promulgated under the authority described in Subtitle VII, Part A, Subpart I, Section 40103. Under that section, the FAA is charged with prescribing regulations to assign the use of the airspace necessary to ensure the safety of aircraft and the efficient use of airspace. This regulation is within the scope of that authority as it modifies terminal airspace as required to preserve the safe and efficient flow of air traffic in the San Juan, PR, area.

History

The FAA published a NPRM for Docket No. FAA-2023-1906 in the **Federal Register** (88 FR 68509; October 4, 2023) proposing to modify the Class C airspace area surrounding SJU. Interested parties were invited to participate in this rulemaking effort by submitting written comments on the proposal. One comment was received from the Air Line Pilots Association International in support of the new SJU Class C airspace design.

Differences From the NPRM

Subsequent to publication of the NPRM, the FAA identified that the SJU Airport Reference Point (ARP) geographic coordinates listed in the Class C airspace description had been rounded in error and published as "lat. 18°26'22" N, long. 66°00'07" W". The correct ARP for SJU is "lat. 18°26'22" N, long. 066°00'08" W". The ARP for SJU is changed from "lat. 18°26'22" N, long. 66°00'07" W" to "lat. 18°26'22" N, long. 066°00'08" W". This final rule corrects the error.

Incorporation by Reference

Class C airspace designations are published in paragraph 4000 of FAA Order JO 7400.11, Airspace Designations and Reporting Points, which is incorporated by reference in 14 CFR 71.1 on an annual basis. This document amends the current version of that order, FAA Order JO 7400.11H, dated August 11, 2023, and effective

September 15, 2023. FAA Order JO 7400.11H is publicly available as listed in the **ADDRESSES** section of this document. This amendment will be published in the next update to FAA Order JO 7400.11.

FAA Order JO 7400.11H lists Class A, B, C, D, and E airspace areas, air traffic service routes, and reporting points.

The Rule

This action amends 14 CFR part 71 by modifying the San Juan Luis Munoz Marin International Airport (SJU), PR, Class C airspace description by adding a cutout to the Class C surface area northwest of SJU from the surface to but not including 1,200 feet above mean sea level (MSL). This amendment enhances flight safety by allowing aircraft departing runway 9 at Fernando Luis Ribas Dominicci Airport, PR (SIG), when the SIG air traffic control tower is closed, the ability to either remain outside of the San Juan, PR, Class C airspace by turning to the north and west or to have additional time to establish two-way radio communication with the San Juan air traffic control tower prior to entering the San Juan, PR, (SJU) Class C airspace.

Additionally, the FAA corrects the first line of the Class C airspace description header information by only listing the city and territory location of the airport. This change follows the FAA's current airspace description format guidance.

Regulatory Notices and Analyses

The FAA considers the impacts of regulatory actions under a variety of executive orders and other requirements. First, Executive Order 12866 and Executive Order 13563 direct that each Federal agency shall propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify the costs. Second, the Regulatory Flexibility Act of 1980 (Pub. L. 96-354) requires agencies to analyze the economic impact of regulatory changes on small entities. Third, the Trade Agreements Act (Pub. L. 96-39) prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. Fourth, the Unfunded Mandates Reform Act of 1995 (Pub. L. 104-4) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate that may result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of \$100,000,000 or more (adjusted annually for inflation) in any one year. The current threshold after

adjustment for inflation is \$177 million using the most current (2022) Implicit Price Deflator for the Gross Domestic Product. This portion of the preamble presents the FAA's analysis of the economic impacts of this rule.

In conducting these analyses, the FAA has determined that this rule: will have a minimal cost impact; is not a "significant regulatory action" as defined in section 3(f)(1) of Executive Order 12866 as amended by Executive Order 14094; will not have a significant economic impact on a substantial number of small entities; will not create unnecessary obstacles to the foreign commerce of the United States; and will not impose an unfunded mandate on State, local, or tribal governments, or on the private sector.

As discussed above, the FAA determined that changes put forth in this final rule will reduce the risk of midair collisions and improve the use of the SJU airspace. The FAA amends the Class C airspace at the San Juan Luis Munoz Marin International Airport (SJU) in Puerto Rico. The existing airspace structure does not adequately address the traffic conflicts that might arise when the SIG Airport Traffic Control Tower (ATCT) is closed, and Visual Flight Rules (VFR) aircraft depart SJU and subsequently transition eastbound through the SJU Class C airspace prior to establishing communications with San Juan air traffic control.

Currently, SIG is considered a satellite airport to SJU, and thus VFR aircraft departing SIG after the SIG ATCT closes only need to contact San Juan air traffic control as soon as practicable, after departing. Traffic conflicts occur when SIG ATCT closes, VFR aircraft depart SIG to the east into SJU Class C airspace and have yet to contact the San Juan air traffic controller. As a result, they could possibly cause midair collisions. The FAA proposes a cutout to the SJU Class C surface area near SIG airport to mitigate the identified safety risks of possible traffic conflicts.

Creating a cutout to the northwest of the SJU Class C surface area allows aircraft coming from the eastern side of SIG to operate without entering the SJU Class C airspace and thus, enhance air traffic efficiency. In addition, the cutout area places the SIG airport outside of the SJC Class C surface area, and therefore, it would require all VFR aircraft departing SIG to contact the San Juan air traffic control prior to entering the SJC Class C airspace area. As a result, it will create a safer airspace.

Regulatory Flexibility Act

The Regulatory Flexibility Act of 1980 (Pub. L. 96-354) (RFA) establishes "as a principle of regulatory issuance that agencies shall endeavor, consistent with the objectives of the rule and of applicable statutes, to fit regulatory and informational requirements to the scale of the businesses, organizations, and governmental jurisdictions subject to regulation." To achieve this principle, agencies are required to solicit and consider flexible regulatory proposals and to explain the rationale for their actions to assure that such proposals are given serious consideration." The RFA covers a wide range of small entities, including small businesses, not-for-profit organizations, and small governmental jurisdictions.

Agencies must perform a review to determine whether a rule will have a significant economic impact on a substantial number of small entities. If the agency determines that it will, the agency must prepare a regulatory flexibility analysis as described in the RFA. However, if an agency determines that a rule is not expected to have a significant economic impact on a substantial number of small entities, section 605(b) of the RFA provides that the head of the agency may so certify, and a regulatory flexibility analysis is not required. The certification must include a statement providing the factual basis for this determination, and the reasoning should be clear.

The final rule amends the Class C airspace at the SJU in Puerto Rico. The FAA is taking this action to reduce the risk of midair collisions and improve the use of the SJU airspace. The FAA determined that changes put forth in this final rule increase airspace safety and efficiency. The change affects general aviation operators using the cutout of SJU Class C surface area when the SIG ATCT is closed, and VFR aircraft depart SIG and subsequently transition eastbound through the SJU Class C airspace prior to establishing communications with San Juan air traffic control. The objectives of these changes are to enhance safety and enable more efficient operations at SJU and SIG without being burdensome to the industry. Therefore, as provided in section 605(b), the head of the FAA certifies that this rulemaking will not result in a significant economic impact on a substantial number of small entities.

International Trade Impact Assessment

The Trade Agreements Act of 1979 (Pub. L. 96-39), as amended by the Uruguay Round Agreements Act (Pub.

L. 103-465), prohibits Federal agencies from establishing standards or engaging in related activities that create unnecessary obstacles to the foreign commerce of the United States. Pursuant to these Acts, the establishment of standards is not considered an unnecessary obstacle to the foreign commerce of the United States, so long as the standard has a legitimate domestic objective, such as the protection of safety, and does not operate in a manner that excludes imports that meet this objective. The statute also requires consideration of international standards and, where appropriate, that they be the basis for U.S. standards. The FAA has assessed the potential effect of this final rule and determined that it should improve safety and is consistent with the Trade Agreements Act. The FAA has assessed the potential effect of this final rule and determined that it will improve safety and is consistent with the Trade Agreements Act.

Unfunded Mandates Assessment

The Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531-1538) governs the issuance of Federal regulations that require unfunded mandates. An unfunded mandate is a regulation that requires a state, local, or tribal government or the private sector to incur direct costs without the Federal government having first provided the funds to pay those costs. The FAA determined that the final rule will not result in the expenditure of \$177 million or more by State, local, or tribal governments, in the aggregate, or the private sector, in any one year. This final rule does not contain such a mandate; therefore, the Act does not apply.

Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)) requires that the FAA consider the impact of paperwork and other information collection burdens imposed on the public. The FAA has determined that there is no new information collection requirement associated with this final rule.

Environmental Review

The FAA has determined that this action of modifying the SJU Class C airspace by adding a cutout to the surface area near the SIG is categorically excluded from further environmental review under the National Environmental Policy Act (42 U.S.C. 4321 *et seq.*) and its implementing regulations at 40 CFR part 1500, and in accordance with FAA Order 1050.1F, Environmental Impacts: Policies and

Procedures, paragraph 5–6.5a, which categorically excludes from further environmental impact review rulemaking actions that designate or modify classes of airspace areas, airways, routes, and reporting points (see 14 CFR part 71, Designation of Class A, B, C, D, and E Airspace Areas; Air Traffic Service Routes; and Reporting Points), and paragraph 5–6.5i, which categorically excludes from further environmental review the establishment of new or revised air traffic control procedures conducted at 3,000 feet or more above ground level (AGL); procedures conducted below 3,000 feet AGL that do not cause traffic to be routinely routed over noise sensitive areas; modifications to currently approved procedures conducted below 3,000 feet AGL that do not significantly increase noise over noise sensitive areas; and increases in minimum altitudes and landing minima, and paragraph 5–6.5k, which categorically excludes from further environmental review the publication of existing air traffic control procedures that do not essentially change existing tracks, create new tracks, change altitude, or change concentration of aircraft on these tracks. As such, this action is not expected to result in any potentially significant environmental impacts. In accordance with FAA Order 1050.1F, paragraph 5–2 regarding Extraordinary Circumstances, the FAA has reviewed this action for factors and circumstances in which a normally categorically excluded action may have a significant environmental impact requiring further analysis. Accordingly, the FAA has determined that no extraordinary circumstances exist that warrant preparation of an environmental assessment or environmental impact study.

List of Subjects in 14 CFR Part 71

Airspace, Incorporation by reference, Navigation (air).

The Amendment

In consideration of the foregoing, the Federal Aviation Administration amends 14 CFR part 71 as follows:

PART 71—DESIGNATION OF CLASS A, B, C, D, AND E AIRSPACE AREAS; AIR TRAFFIC SERVICE ROUTES; AND REPORTING POINTS

■ 1. The authority citation for 14 CFR part 71 continues to read as follows:

Authority: 49 U.S.C. 106(f), 106(g), 40103, 40113, 40120; E.O. 10854, 24 FR 9565, 3 CFR, 1959–1963 Comp., p. 389.

§ 71.1 [Amended]

■ 2. The incorporation by reference in 14 CFR 71.1 of FAA Order JO 7400.11H, Airspace Designations and Reporting Points, dated August 11, 2023, and effective September 15, 2023, is amended as follows:

Paragraph 4000. Class C Airspace.

* * * * *

ASO PR C San Juan, PR [Amended]

Luis Munoz Marin International Airport, PR (Lat. 18°26'22" N, long. 066°00'08" W)

That airspace extending upward from the surface to and including 4,000 feet MSL within a 5-mile radius of the Luis Munoz Marin International Airport beginning at lat. 18°30'24" N, long. 066°03'16" W, clockwise to lat. 18°26'41" N, long. 066°05'23" W, thence east to lat. 18°26'42" N, long. 066°03'34" W, thence north to the beginning point; and that airspace extending upward from 2,800 feet MSL to 4,000 feet MSL within a 10-mile radius of the Luis Munoz Marin International Airport from the 129° bearing from the airport clockwise to the 189° bearing from the airport; and that airspace extending upward from 1,700 feet MSL to 4,000 feet MSL within a 10-mile radius of the airport from the 189° bearing from the airport clockwise to the 229° bearing from the airport; and that airspace extending upward from 1,200 feet MSL to 4,000 feet MSL within a 10-mile radius of the airport from the 229° bearing from the airport clockwise to the 129° bearing from the airport.

* * * * *

Issued in Washington, DC, on March 29, 2024.

Frank Lias,

Manager, Rules and Regulations Group.

[FR Doc. 2024–07086 Filed 4–3–24; 8:45 am]

BILLING CODE 4910–13–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Part 165

[Docket Number USCG–2024–0204]

RIN 1625–AA00

Safety Zone; Kokosing ROV Survey Operation, Straits of Mackinac, MI

AGENCY: Coast Guard, DHS.

ACTION: Temporary final rule.

SUMMARY: The Coast Guard is establishing a temporary safety zone for navigable waters within a 500-yard radius of Tug Nancy Anne, Tug Champion, Tug General, Tug WM Boyd, Tug Shirley Ann and crew boat Timmy V. The safety zone is needed to protect the remotely operated vehicle survey operations from other vessels. Entry of

vessels into this zone is prohibited unless specifically authorized by the Captain of the Port Northern Great Lakes.

DATES: This rule is effective without actual notice from April 4, 2024 through May 15, 2024. For the purposes of enforcement, actual notice will be used from April 1, 2024 until April 4, 2024.

ADDRESSES: To view documents mentioned in this preamble as being available in the docket, go to <https://www.regulations.gov>, type USCG–2024–0204 in the search box and click “Search.” Next, in the Document Type column, select “Supporting & Related Material.”

FOR FURTHER INFORMATION CONTACT: If you have questions about this rulemaking, call or email LT Rebecca Simpson, telephone 906–635–3223, email ssmprevention@uscg.mil.

SUPPLEMENTARY INFORMATION:

I. Table of Abbreviations

CFR Code of Federal Regulations
DHS Department of Homeland Security
FR Federal Register
NPRM Notice of proposed rulemaking
§ Section
U.S.C. United States Code
ROV Remotely Operated Vehicle

II. Background Information and Regulatory History

The Coast Guard is issuing this temporary rule under authority in 5 U.S.C. 553(b)(B). This statutory provision authorizes an agency to issue a rule without prior notice and opportunity to comment when the agency for good cause finds that those procedures are “impracticable, unnecessary, or contrary to the public interest.” The Coast Guard finds that good cause exists for not publishing a notice of proposed rulemaking (NPRM) with respect to this rule because it is impracticable to publish an NPRM because we must establish this safety zone by April 1, 2024.

Also, under 5 U.S.C. 553(d)(3), the Coast Guard finds that good cause exists for making this rule effective less than 30 days after publication in the **Federal Register**. This rule is needed to protect the vessels and personnel involved in the ROV survey operations from other vessels transiting the Straits of Mackinac at the same time this project is being conducted.

III. Legal Authority and Need for Rule

The Coast Guard is issuing this rule under authority in 46 U.S.C. 70034. The Captain of the Port Sector Northern Great Lakes (COTP) has determined that potential hazards associated with the

ROV survey starting April 1, 2024, will be a safety concern for anyone within a 500-yard radius of the equipment, including Tug Nancy Anne, Tug Champion, Tug General, Tug WM Boyd, Tug Shirley Ann and crew boat Timmy V. This rule is needed to protect personnel, vessels, and the marine environment in the navigable waters within the safety zone while the stone laying operation is being conducted.

IV. Discussion of the Rule

This rule establishes a safety zone from April 1, 2024 through May 15, 2024. The safety zone will cover all navigable waters within 500 yards of Tug Nancy Anne, Tug Champion, Tug General, Tug WM Boyd, Tug Shirley Ann and crew boat Timmy V. The duration of the safety zone is intended to protect personnel and vessels involved with conducting the ROV survey operations. No vessel or person will be permitted to enter the safety zone without obtaining permission from the COTP.

V. Regulatory Analyses

We developed this rule after considering numerous statutes and Executive orders related to rulemaking. Below we summarize our analyses based on a number of these statutes and Executive orders, and we discuss First Amendment rights of protestors.

A. Regulatory Planning and Review

Executive Orders 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits. This rule has not been designated a “significant regulatory action,” under section 3(f) of Executive Order 12866, as amended by Executive Order 14094 (Modernizing Regulatory Review). Accordingly, this rule has not been reviewed by the Office of Management and Budget (OMB).

This regulatory action determination is based on the size and location of the safety zone. Vessel traffic will be able to safely transit around this safety zone which would impact a small designated area of the Straits of Mackinac. Moreover, the Coast Guard will issue a Local Notice to Mariners about the safety zone, and the rule would allow vessels to seek permission to enter the zone.

B. Impact on Small Entities

The Regulatory Flexibility Act of 1980, 5 U.S.C. 601–612, as amended, requires Federal agencies to consider the potential impact of regulations on

small entities during rulemaking. The term “small entities” comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. The Coast Guard certifies under 5 U.S.C. 605(b) that this rule will not have a significant economic impact on a substantial number of small entities.

While some owners or operators of vessels intending to transit the safety zone may be small entities, for the reasons stated in section V.A above, this rule would not have a significant economic impact on any vessel owner or operator.

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104–121), we want to assist small entities in understanding this rule. If the rule would affect your small business, organization, or governmental jurisdiction and you have questions concerning its provisions or options for compliance, please call or email the person listed in the **FOR FURTHER INFORMATION CONTACT** section.

Small businesses may send comments on the actions of Federal employees who enforce, or otherwise determine compliance with, Federal regulations to the Small Business and Agriculture Regulatory Enforcement Ombudsman and the Regional Small Business Regulatory Fairness Boards. The Ombudsman evaluates these actions annually and rates each agency’s responsiveness to small business. If you wish to comment on actions by employees of the Coast Guard, call 1–888–REG–FAIR (1–888–734–3247). The Coast Guard will not retaliate against small entities that question or complain about this rule or any policy or action of the Coast Guard.

C. Collection of Information

This rule will not call for a new collection of information under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501–3520).

D. Federalism and Indian Tribal Governments

A rule has implications for federalism under Executive Order 13132, Federalism, if it has a substantial direct effect on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government. We have analyzed this rule under that Order and have determined that it is consistent with the fundamental federalism

principles and preemption requirements described in Executive Order 13132.

Also, this rule does not have tribal implications under Executive Order 13175, Consultation and Coordination with Indian Tribal Governments, because it does not have a substantial direct effect on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes.

E. Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531–1538) requires Federal agencies to assess the effects of their discretionary regulatory actions. In particular, the Act addresses actions that may result in the expenditure by a State, local, or tribal government, in the aggregate, or by the private sector of \$100,000,000 (adjusted for inflation) or more in any one year. Though this rule will not result in such an expenditure, we do discuss the effects of this rule elsewhere in this preamble.

F. Environment

We have analyzed this rule under Department of Homeland Security Directive 023–01, Rev. 1, associated implementing instructions, and Environmental Planning COMDTINST 5090.1 (series), which guide the Coast Guard in complying with the National Environmental Policy Act of 1969 (42 U.S.C. 4321–4370f), and have made a preliminary determination that this action is one of a category of actions that do not individually or cumulatively have a significant effect on the human environment. This rule involves all vessels. Normally such actions are categorically excluded from further review under paragraph L[60a] of Appendix A, Table 1 of DHS Instruction Manual 023–01–001–01, Rev. 1. We seek any comments or information that may lead to the discovery of a significant environmental impact from this rule.

G. Protest Activities

The Coast Guard respects the First Amendment rights of protesters. Protesters are asked to call or email the person listed in the **FOR FURTHER INFORMATION CONTACT** section to coordinate protest activities so that your message can be received without jeopardizing the safety or security of people, places, or vessels.

List of Subjects in 33 CFR Part 165

Harbors, Marine safety, Navigation (water), Reporting and recordkeeping

requirements, Security measures, Waterways.

For the reasons discussed in the preamble, the Coast Guard amends 33 CFR part 165 as follows:

PART 165—REGULATED NAVIGATION AREAS AND LIMITED ACCESS AREAS

■ 1. The authority citation for part 165 continues to read as follows:

Authority: 46 U.S.C. 70034, 70051, 70124; 33 CFR 1.05–1, 6.04–1, 6.04–6, and 160.5; Department of Homeland Security Delegation No. 00170.1, Revision No. 01.3.

■ 2. Add § 165.T09–0207 to read as follows:

§ 165.T09–0207 Safety Zone; Tugs Nancy Anne, Champion, General, WM Boyd, Shirley Ann, and crew boat Timmy V operating in the Straits of Mackinac, MI.

(a) *Location.* The following areas are safety zones: All navigable water within 500 yards of the Tugs Nancy Anne, Champion, General, WM Boyd, Shirley Ann, and crew boat Timmy V while conducting ROV survey operations within one nautical mile of charted submerged pipeline or cable within the Straits of Mackinac RNA.

(b) *Definitions.* As used in this section, designated representative means a Coast Guard Patrol Commander, including a Coast Guard coxswain, petty officer, or other officer operating a Coast Guard vessel and a Federal, State, and local officer designated by or assisting the Captain of the Port Northern Great Lakes (COTP) in the enforcement of the safety zone.

(c) *Regulations.* (1) Under the general safety zone regulations in subpart D of this part, you may not enter the safety zone described in paragraph (a) of this section unless authorized by the COTP or the COTP's designated representative.

(2) To seek permission to enter, contact the COTP or the COTP's representative by VHF Channel 16 or telephone at (906) 635–3233. Those in the safety zone must comply with all lawful orders or directions given to them by the COTP or the COTP's designated representative.

(d) *Enforcement period.* This section will be enforced from 12:01 a.m. April 1, 2024, through 11:59 p.m. on May 15, 2024.

Dated: March 29, 2024.

J.R. Bendle,

Captain, U.S. Coast Guard, Captain of the Port Sector Northern Great Lakes.

[FR Doc. 2024–07079 Filed 4–3–24; 8:45 am]

BILLING CODE 9110–04–P

DEPARTMENT OF EDUCATION

34 CFR Chapter VI

[ED–2024–OPE–0002]

Augustus F. Hawkins Centers of Excellence Program

AGENCY: Office of Postsecondary Education, Department of Education.

ACTION: Final priorities, requirements, and definition.

SUMMARY: The Department of Education (Department) issues priorities, requirements, and definition for use in the Augustus F. Hawkins Centers of Excellence (Hawkins) Program, Assistance Listing Number 84.428A. The Department may use one or more of these priorities, requirements, and definition for competitions in fiscal year (FY) 2024 and later years. We intend for these priorities, requirements, and definition to help increase the number of, and retain, well-prepared teachers from diverse backgrounds, resulting in a more diverse teacher workforce prepared to teach in our Nation's underserved elementary and secondary schools and close student opportunity and achievement gaps.

DATES: These priorities, requirements, and definition are effective May 6, 2024.

FOR FURTHER INFORMATION CONTACT: Dr. Vicki Robinson, U.S. Department of Education, 400 Maryland Avenue SW, 5th floor, Washington, DC 20202. Telephone: (202) 453–7907. Email: Vicki.Robinson@ed.gov. You may also contact Ashley Hillary, U.S. Department of Education, 400 Maryland Avenue SW, 5th floor, Washington, DC 20202. Telephone: (202) 453–7880. Email: Ashley.Hillary@ed.gov.

If you are deaf, hard of hearing, or have a speech disability and wish to access telecommunications relay services, please dial 7–1–1.

SUPPLEMENTARY INFORMATION:

Purpose of Program: The Hawkins Program, authorized under Part B of Title II of the Higher Education Act of 1965, as amended (HEA), is designed to support comprehensive, high-quality State-accredited teacher preparation programs by creating centers of excellence at Historically Black Colleges and Universities (HBCUs); Tribal Colleges or Universities (TCUs); or Minority Serving Institutions (MSIs), such as Hispanic-Serving Institutions (HSIs). The Hawkins Program will help increase the number of, and retain, well-prepared teachers from diverse backgrounds, resulting in a more diverse teacher workforce prepared to teach in our Nation's most-underserved

elementary and secondary schools and close student opportunity and achievement gaps. This program focuses on the various aspects of the teacher preparation pipeline, including the recruitment, preparation, support, placement, retention and retraining of teachers for and in under-resourced schools to support underserved students. Through this program, the Secretary seeks to fund applicants that propose to incorporate evidence-based practices into their teacher preparation program.

Program Authority: 20 U.S.C. 1033–1033a.

We published a notice of proposed priorities, requirements, and definition in the **Federal Register** on February 1, 2024 (89 FR 6470) (NPP). That document contained background information and the Department's reasons for proposing the particular priorities, requirements, and definition. There are no substantive differences between the proposed priorities, requirements, and definition and these final priorities, requirements, and definition.

Public Comment: In response to our invitation in the NPP, six parties submitted comments on the proposed priorities, requirements, and definition. Generally, we do not address technical and other minor changes, or suggested changes that the law does not authorize us to make under applicable statutory authority. In addition, we do not address general comments that raised concerns not directly related to the proposed priorities, requirements, or definition.

Analysis of Comments and Changes: An analysis of the comments and of any changes in the priorities, requirements, and definition since publication of the NPP follows.

General Comments

Comments: Two commenters expressed support for components from several of the proposed priorities, including the emphasis on evidence-based components of teacher preparation programs, the focus on clinical experiences and high-quality mentoring, the support for teacher candidates serving in schools in roles that assist students and teachers, the recognition that the retention and preparation of teacher candidates from diverse backgrounds benefits all students, and the use of HBCUs, TCUs, and MSIs to prepare teachers. One commenter expressed support for the definition of “pre-service.”

Discussion: We appreciate the support of the priorities and the definition.

Changes: None.

Comments: One commenter asked us to expand Priority 2 to include teacher candidates with disabilities.

Discussion: Priority 2 is designed to increase teacher diversity by supporting teacher candidates from backgrounds that are underrepresented in the profession, which could include teacher candidates with disabilities. Applicants under this priority are asked for a plan to identify, support, and promote the retention of teacher candidates “from backgrounds that are underrepresented in the profession.” While teacher candidates of color are mentioned as one such population of individuals underrepresented within the teaching profession, under this priority, applicants may propose to serve individuals from other underrepresented populations, including but not limited to teacher candidates with disabilities. This is consistent with the authorizing statute for this program, which incorporates as an allowable use of funds “consideration of individuals from underrepresented populations in the teaching profession.” 20 U.S.C. 1022a(e)(2)(a)(vi)(II).

Changes: None.

Comments: One commenter asked that we include a priority to support early childhood multilingual teacher preparation pathways.

Discussion: We agree that there is a need for supports for bilingual and multilingual teachers, including for early learners. Priority 3 is designed to expand the number of bilingual and multilingual teachers with full teacher certification. For purposes of this grant program, this priority is focused on increasing the number of teachers across elementary and secondary schools who are fully certified to provide academic language instruction in a language other than English, including for English Learners (ELs), because of the focus within 20 U.S.C. 1033a(b)(2) on teacher preparation for elementary and secondary schools. While we are not including it as a priority, projects to support pathways for early childhood teachers would be permitted under this program.

Changes: None.

Comments: One commenter contended that the Hawkins grant program overall is discriminatory.

Discussion: We disagree with the commenter. The program does not discriminate against any group. The authorizing statute for this program incorporates as an allowable use of funds “consideration of individuals from underrepresented populations in the teaching profession.” 20 U.S.C. 1022a(e)(2)(a)(vi)(II). As such, Priority 2

is designed to increase the number of well-prepared teachers and the diversity of the teacher workforce by seeking supports for teacher candidates and teachers from backgrounds that are underrepresented in the profession. In addressing this priority, applicants will be able to identify specific populations that are underrepresented in the teaching profession across a range of characteristics, and the priority language does not prohibit teacher candidates who are not from underrepresented populations from participating in the project.

Changes: None.

Comments: One commenter expressed concerns with linking closure of the achievement gap to teacher diversity.

Discussion: The statutory purpose of the Hawkins grant program is to support teacher preparation programs that “prepare teachers to serve in low-performing schools and close student achievement gaps.” 20 U.S.C. 1033a(b)(1)(B)(i). We believe, based on current research, that increasing the number of well-prepared teachers from diverse backgrounds is one factor that can contribute to the success of students. Research shows that teachers of color benefit all students and can have a significant positive impact on students of color,¹ including higher levels of student achievement.² Additionally, as we discussed in the NPP, and as the commenter recognizes, there are numerous reasons students benefit from a diverse teacher workforce.

Changes: None.

Final Priorities

The Secretary establishes the following priorities for use in the Hawkins Program.

Priority 1: Increase Evidence-Based, Comprehensive Pre-service Clinical Experiences Through Teacher Preparation Programs.

Under this priority, an eligible applicant must propose projects that are evidence-based (as defined in 34 CFR 77.1) comprehensive teacher preparation programs that provide extensive clinical experience. Applicants with existing programs must describe their record in graduating highly skilled, well-prepared, and

diverse teachers and describe how the proposed project will refine or enhance existing programs. Applicants proposing new programs must describe how their new program is evidence-based and designed to achieve the intended outcomes of the Hawkins Program. Applicants must also address how they will—

(a) Examine the sources of inequity and inadequacy in resources and opportunity and implement pedagogical practices in teacher preparation programs that are inclusive with regard to race, ethnicity, culture, language, gender, and disability status and that prepare teachers to create inclusive, supportive, equitable, unbiased, and identity-safe learning environments for their students;

(b) Prepare teacher candidates to integrate rigorous academic content, including through the effective use of technology, and instructional techniques and strategies consistent with universal design for learning principles;

(c) Prepare teacher candidates to design and deliver instruction in ways that are engaging and provide their students with opportunities to think critically and solve complex problems, apply learning in authentic and real-world settings, communicate and collaborate effectively, and develop growth mindsets. Teacher candidate pedagogy should include how to incorporate project-based, work-based, or other experiential learning opportunities in curriculum development;

(d) Prepare teacher candidates to build meaningful and trusting relationships with students and their families to support in-home, community-based, and in-school learning; and

(e) Provide sustained and high-quality pre-service clinical experiences, including teaching assistant initiatives, that facilitate the pathway to the teaching credential for those with paraprofessional experience or high-quality school leader pre-service training, induction, and support in the first three years of school leadership for principals and other school leaders. In designing such experiences, applicants must consider opportunities to provide pre-service clinical experience earlier in the teacher preparation program, as is practicable, and in ways that benefit students and teachers. These clinical experiences must be designed to—

(1) Integrate pedagogy and classroom practice and promote effective teaching skills in academic content areas;

¹ Dee, T. (2004). Teachers, race and student achievement in a randomized experiment. *The Review of Economics and Statistics*, 86(1), 195–210; Gershenson, S., Hart, C.M.D., Lindsay, C.A., & Papageorge, N.W. (2017). *The long-run impacts of same race teachers*. Bonn, Germany: IZA Institute of Labor Economics. Discussion Paper Series

² Egalite, A., Kisida, B., & Winters, M.A. Representation in the classroom: The effect of own-race teachers on student achievement. *Economics of Education Review*, 45 (April 2015), 44–52.

(2) Be tightly aligned with course work with clear, relevant, and strong links between theory and practice;

(3) Group teacher candidates in cohorts to facilitate reflection of practice and professional collaboration;

(4) Closely supervise interaction between teacher candidates and faculty, experienced teachers, principals, and other administrators in high-need schools or hard-to-staff schools; and

(5) Provide high-quality-teacher mentoring.

Priority 2: Projects that are Designed to Increase and Retain the Number of Well-Prepared Teachers from Diverse Backgrounds.

Under this priority, applicants must propose projects that are designed to increase the number of well-prepared teachers and the diversity of the teacher workforce with a focus on increasing and retaining a diverse teacher workforce, and improving the preparation, recruitment, retention, and placement of such teachers.

Applicants addressing this priority must describe—

(a) How their project will integrate multiple services or initiatives across academic and student affairs, such as academic advising, counseling, stipends, child-care, structured/guided pathways from teacher candidates' first year in the preparation program through successful employment placement, career services, or student financial aid, such as scholarships, with the goal of increasing program completion and credential attainment;

(b) Their plan for identifying and supporting teacher candidates from backgrounds that are underrepresented in the profession, including teacher candidates of color. This plan must span the beginning of the preparation program through graduation, and include a plan to improve program entry rates, as applicable, graduation rates, passage rates for certification and licensure exams, and rates of successful employment placement between teacher candidate subgroups and an institution's overall teacher candidate population; and

(c) Their proposed initiatives to promote the retention of teachers from backgrounds that are underrepresented in the profession, including teachers of color, prepared through the program, which may include induction programs, such as teacher or school leader induction programs, or mentorship programs that provide school and district leaders with the support they need to persist in their professions.

Priority 3—Increasing the Number of Bilingual and/or Multilingual Teachers with Full Certification.

Under this priority, applicants must propose projects that are designed to prepare effective and experienced bilingual and/or multilingual teachers for high-need schools by increasing the number of teachers across elementary and secondary schools who are fully certified to provide academic language instruction in a language other than English, including for English Learners (ELs). These projects must prepare teacher candidates to lead students toward linguistic fluency and academic achievement in more than one language. Applicants must describe—

(a) How their project will integrate multiple services or initiatives across academic and student affairs, such as academic advising, counseling, stipends, child-care, structured/guided pathways from teacher candidates' first year in the preparation program through successful employment placement, career services, or student financial aid, such as scholarships, and provide the necessary knowledge and skills so that teacher candidates can serve students from many different language backgrounds; and

(b) Their plan for recruiting, supporting, and retaining bilingual and/or multilingual teacher candidates, including those who may have a teaching credential but have not been teaching in bilingual and/or multilingual education settings; aspiring teachers; and teaching assistants who are interested in becoming bilingual and/or multilingual teachers.

Types of Priorities

When inviting applications for a competition using one or more priorities, we designate the type of each priority as absolute, competitive preference, or invitational through a notice in the **Federal Register**. The effect of each type of priority follows:

Absolute priority: Under an absolute priority, we consider only applications that meet the priority (34 CFR 75.105(c)(3)).

Competitive preference priority: Under a competitive preference priority, we give competitive preference to an application by (1) awarding additional points, depending on the extent to which the application meets the priority (34 CFR 75.105(c)(2)(i)); or (2) selecting an application that meets the priority over an application of comparable merit that does not meet the priority (34 CFR 75.105(c)(2)(ii)).

Invitational priority: Under an invitational priority, we are particularly interested in applications that meet the priority. However, we do not give an application that meets the priority a

preference over other applications (34 CFR 75.105(c)(1)).

Final Requirements

The Secretary establishes the following requirements for use in the Hawkins Program.

Requirement 1—Draft Written Agreement with Clinical Practice Partner(s). An applicant must provide a Draft Written Agreement (DWA) that identifies the partnership between: (1) at least one eligible IHE with a State accredited teacher preparation program, and (2) a high-need local educational agency (LEA) or consortium of high-need LEAs, or with a high-need school or consortium of high-need schools. The agreement with partners is intended to ensure that the parties joining the project are committed to fulfilling the purpose of the clinical practice by either creating new partnerships or expanding existing partnerships, and that teacher candidates will not become the teacher of record prior to completing the certification program, including pre-service clinical experience, and, for any candidates who entered the program without a bachelor's degree, obtaining a bachelor's. Grantees will finalize the DWA into a Final Written Agreement (FWA) within 120 days of grant award notification.

Requirement 2—Supplement-Not-Supplant. Grant funds must be used so that they supplement and, to the extent practical, increase the funds that would otherwise be available for the activities to be carried out under this grant.

Requirement 3—Indirect Cost Rate Information. A grantee's indirect cost reimbursement is limited to 8 percent of a modified total direct cost base. For more information regarding indirect costs, or to obtain a negotiated indirect cost rate, please see www.ed.gov/about/offices/list/ocfo/intro.html.

Final Definition

The Secretary establishes the following definition for use in the Hawkins Program.

Pre-service means the period of training for a person who does not have a prior teaching certification or license and who is enrolled in a State-approved teacher education program at an institution of higher education, prior to becoming the teacher of record.

This document does not preclude us from proposing additional priorities, requirements, definitions, or selection criteria, subject to meeting applicable rulemaking requirements.

Note: This document does *not* solicit applications. In any year in which we choose to use any of these priorities, requirements, or definition, we invite

applications through a notice in the **Federal Register**.

Executive Orders 12866, 13563, and 14094

Regulatory Impact Analysis

Under Executive Order 12866, the Office of Management and Budget (OMB) determines whether this regulatory action is “significant” and, therefore, subject to the requirements of the Executive order and subject to review by OMB. Section 3(f) of Executive Order 12866, as amended by Executive Order 14094, defines a “significant regulatory action” as an action likely to result in a rule that may—

(1) Have an annual effect on the economy of \$200 million or more (adjusted every three years by the Administrator of Office of Information and Regulatory Affairs (OIRA) for changes in gross domestic product); or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, territorial, or Tribal governments or communities;

(2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another agency;

(3) Materially alter the budgetary impacts of entitlements, grants, user fees, or loan programs or the rights and obligations of recipients thereof; or

(4) Raise legal or policy issues for which centralized review would meaningfully further the President’s priorities, or the principles set forth in this Executive order, as specifically authorized in a timely manner by the Administrator of OIRA in each case.

This final regulatory action is not a significant regulatory action subject to review by OMB under section 3(f) of Executive Order 12866, as amended by Executive Order 14094.

We have also reviewed this final regulatory action under Executive Order 13563, which supplements and explicitly reaffirms the principles, structures, and definitions governing regulatory review established in Executive Order 12866, as amended by Executive Order 14094. To the extent permitted by law, Executive Order 13563 requires that an agency—

(1) Propose or adopt regulations only upon a reasoned determination that their benefits justify their costs (recognizing that some benefits and costs are difficult to quantify);

(2) Tailor its regulations to impose the least burden on society, consistent with obtaining regulatory objectives and taking into account—among other things

and to the extent practicable—the costs of cumulative regulations;

(3) In choosing among alternative regulatory approaches, select those approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distributive impacts; and equity);

(4) To the extent feasible, specify performance objectives, rather than the behavior or manner of compliance a regulated entity must adopt; and

(5) Identify and assess available alternatives to direct regulation, including economic incentives—such as user fees or marketable permits—to encourage the desired behavior, or provide information that enables the public to make choices.

Executive Order 13563 also requires an agency “to use the best available techniques to quantify anticipated present and future benefits and costs as accurately as possible.” The Office of Information and Regulatory Affairs of OMB has emphasized that these techniques may include “identifying changing future compliance costs that might result from technological innovation or anticipated behavioral changes.”

We are issuing these final priorities, requirements, and definition only on a reasoned determination that their benefits justify their costs. In choosing among alternative regulatory approaches, we selected those approaches that maximize net benefits. Based on the analysis that follows, the Department believes that this regulatory action is consistent with the principles in Executive Order 13563.

The potential costs associated with these priorities, requirements, and definition are minimal, while the potential benefits are significant. The Department believes that this final regulatory action will not impose significant costs on eligible entities. Participation in this program is voluntary, and the costs imposed on applicants by this regulatory action will be limited to paperwork burden related to preparing an application. The potential benefits of implementing the program will outweigh the costs incurred by applicants, and the costs of carrying out activities associated with the application will be paid for with program funds. For these reasons, we have determined that the costs of implementation will not be burdensome for eligible applicants, including small entities.

We also have determined that this regulatory action does not unduly interfere with State, local, and Tribal

governments in the exercise of their governmental functions.

In accordance with these Executive orders, the Department has assessed the potential costs and benefits, both quantitative and qualitative, of this regulatory action. The potential costs are those resulting from statutory requirements and those we have determined as necessary for administering the Department’s programs and activities.

Intergovernmental Review: This program is subject to Executive Order 12372 and the regulations in 34 CFR part 79. One of the objectives of the Executive order is to foster an intergovernmental partnership and a strengthened federalism. The Executive order relies on processes developed by State and local governments for coordination and review of Federal financial assistance.

This document provides early notification of our specific plans and actions for this program.

Regulatory Flexibility Act Certification

The Secretary certifies that these final priorities, requirements, and definition will not have a significant economic impact on a substantial number of small entities.

The small entities that this final regulatory action will affect are IHEs that meet the eligibility requirements described in section 241(1) of the HEA. The Secretary believes that the costs imposed on applicants by the final priorities, requirements, and definition will be limited to paperwork burden related to preparing an application and that the benefits will outweigh any costs incurred by applicants. Participation in this program is voluntary. For this reason, the final priorities, requirements, and definition will impose no burden on small entities unless they applied for funding under the program. We expect that in determining whether to apply for Hawkins Program funds, an eligible applicant would evaluate the requirements of preparing an application and any associated costs, and weigh them against the benefits likely to be achieved by receiving a Hawkins Program grant. Eligible applicants most likely would apply only if they determine that the likely benefits exceed the costs of preparing an application. The likely benefits include the potential receipt of a grant as well as other benefits that may accrue to an entity through its development of an application, such as the use of that application to seek funding from other sources to address the teacher shortage

present in the Nation's high need-need public schools.

This final regulatory action will not have a significant economic impact on a small entity once it receives a grant because it will be able to meet the costs of compliance using the funds provided under this program.

Paperwork Reduction Act of 1995

These final priorities, requirements, and definition do not contain any information collection requirements.

Accessible Format: On request to the program contact person listed under **FOR FURTHER INFORMATION CONTACT**, individuals with disabilities can obtain this document in an accessible format. The Department will provide the requestor with an accessible format that may include Rich Text Format (RTF) or text format (txt), a thumb drive, an MP3 file, braille, large print, audiotape, or compact disc, or other accessible format.

Electronic Access to This Document: The official version of this document is the document published in the **Federal Register**. You may access the official edition of the **Federal Register** and the Code of Federal Regulations at www.govinfo.gov. At this site you can view this document, as well as all other documents of this Department published in the **Federal Register**, in text or Portable Document Format (PDF). To use PDF you must have Adobe Acrobat Reader, which is available free at the site.

You may also access documents of the Department published in the **Federal Register** by using the article search feature at www.federalregister.gov. Specifically, through the advanced search feature at this site, you can limit your search to documents published by the Department.

Nasser Paydar,

Assistant Secretary for Postsecondary Education.

[FR Doc. 2024-07131 Filed 4-3-24; 8:45 am]

BILLING CODE 4000-01-P

DEPARTMENT OF VETERANS AFFAIRS

38 CFR Part 17

Instructions for Determining Eligibility for In Vitro Fertilization (IVF) Benefit

AGENCY: Department of Veterans Affairs.

ACTION: General policy statement.

SUMMARY: The Department of Veterans Affairs (VA) announces that the Secretary of Veterans Affairs issued Instruction of the Secretary 01-24 on March 28, 2024, which addresses the

expansion of eligibility for IVF benefits to qualified Veterans and their spouses. VA's authority to provide assisted reproductive technology (ART) benefits to veterans and their spouses, including IVF coverage, references the benefits the Department of Defense (DoD) provides to active-duty service members. The primary benefit provided by VA under this authority is IVF. DoD previously limited the IVF benefit to service members who had a Category II or III injury or illness and who together with their legal spouse could produce and carry a child who is biologically their own. This limitation effectively limited the benefit to service members who were legally married and capable of producing their own sperm and eggs (gametes) within that marriage. On March 8, 2024, DoD amended its policy to cover IVF for service members with a qualifying injury or illness who are unmarried and to allow donated gametes and embryos. VA is amending its IVF policy to adopt conforming changes.

DATES: Instructions for Determining Eligibility for IVF Benefit is effective March 28, 2024.

FOR FURTHER INFORMATION CONTACT: Sally G. Haskell, MD, MS, Acting Chief Officer, Office of Women's Health, Veterans Health Administration, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420, 202-461-0373. (This is not a toll-free number.)

SUPPLEMENTARY INFORMATION: Instruction of the Secretary 01-24 Notice is given that the Secretary of Veterans Affairs issued Instruction of the Secretary 01-24—Instructions for Determining Eligibility for In Vitro Fertilization (IVF) Benefit on March 28, 2024. The text of Instruction of the Secretary 01-24 appears at the end of this **Federal Register** document.

Background

On April 3, 2012, DoD implemented its IVF policy in a memorandum titled "Policy for Assisted Reproductive Services for the Benefit of Seriously or Severely Ill/Injured (Category II or III) Active Duty Service Members," accompanied by implementation guidance (collectively referred to throughout this document as the "DoD Policy"). The DoD Policy restricted the benefit to service members with a qualifying injury or illness who, together with their legal spouse, were able to produce and carry a child who is biologically their own. This effectively limited the benefit to service members who were legally married and capable of producing a child who is

biologically related to the service member and their spouse.

Since 2016, Congress has authorized VA to use medical services funds to provide ART benefits, which includes IVF coverage, to covered veterans or to provide fertility treatment services including ART to the spouses of covered veterans as provided to a member of the Armed Forces under the DoD Policy. Public Law 114-223, Division A, Title II, section 260 (Sept. 29, 2016). Congress defined a "covered veteran" to be one who has a service-connected disability that results in the inability of the veteran to procreate without the use of fertility treatment. Congress has continued to reauthorize the use of medical services funds for this purpose in subsequent appropriations laws, most recently in March 2024 in Public Law 118-42, Division A, Title II, section 234.

VA implemented Congress's authorization by issuing 38 CFR 17.380 and 17.412, which clarified the definition of a covered veteran for the purposes of establishing eligibility for IVF coverage and authorized fertility treatment of the legal spouse of a covered veteran, respectively. VA also issued VHA Directive 1334 establishing the full eligibility criteria for IVF coverage, including the applicable restrictions contained in the DoD Policy.

On March 8, 2024, DoD amended the DoD Policy to eliminate the requirement that to receive IVF and other ART services, an active-duty service member, along with their legal spouse, be able to produce and carry a child who is biologically their own. In the amended policy, DoD expressly stated that eligibility would not be based on marital status and that donor sperm, eggs, and embryos may be used in ART services, including IVF.

VHA Directive 1334, paragraph 1.c. provides that any substantive changes made to DoD's policy will supersede conflicting terms in VHA Directive 1334. Therefore, in Instruction of the Secretary 01-24, issued on March 28, 2024, the Secretary has directed VA employees and officials to revise VHA Directive 1334 to eliminate the requirement that a covered veteran to be married and be able to produce and carry a child who is biologically their own in order to qualify for IVF coverage. These revisions allow VA to provide IVF services for an unmarried covered veteran. The revisions also allow for the use of donor sperm, eggs, or embryos, as long as the donated sperm, eggs, and embryos are provided at no cost to VA. Effectively, the revisions to VHA Directive 1334 allow VA to expand the provision of IVF services to covered veterans who are unmarried, married to

a partner who does not have opposite-sex gametes, and/or incapable of producing their own sperm and/or eggs.

Instruction of the Secretary 01–24 does not eliminate the statutorily imposed requirement that a veteran must have a service-connected disability that results in the inability of the veteran to procreate without the use of fertility treatment to be considered a “covered veteran.” However, the Instruction clarifies that the definition of “a service-connected disability that results in the inability of the veteran to procreate without the use of fertility treatment” provided for female veterans who have ovarian function and a patent uterine cavity in 38 CFR 17.380 will also apply to female veterans without ovarian function or a patent uterine cavity. Previously, no definition was provided for the female veteran population that did not have ovarian function or a patent uterine cavity because the exclusion of donor sperm, eggs, and embryos eliminated them from eligibility. Now, the Secretary clarifies they must meet the same definition as female veteran with ovarian function and a patent uterine cavity to be considered a “covered veteran.”

Text of Instruction of Secretary 01–24
MEMORANDUM FOR THE UNDER SECRETARY FOR HEALTH AND THE CHAIRMAN, BOARD OF VETERANS APPEALS

Subject: Instructions for Determining Eligibility for In Vitro Fertilization (IVF) Benefit.

Purpose

1. I am issuing this instruction to clarify the impact for the Department of Veterans Affairs (VA or the Department) of the amendment to the Department of Defense (DoD) Policy for Assisted Reproductive Services (ART) for the Benefit of Seriously or Severely Ill/Injured (Category II or III) Active Duty Service Members (hereinafter referred to as the “DoD Policy”) issued by DoD on March 8, 2024. The amendments to the DoD Policy are substantive and have superseded the conflicting terms of VHA Directive 1334(1), In Vitro Fertilization Counseling and Services Available to Certain Eligible Veterans and Their Spouses, dated March 21, 2021, in accordance with paragraph 1.c. of that Directive.

2. I am instructing VA employees to not restrict eligibility for IVF services based on marital status or the ability to produce opposite-sex autologous gametes, as described in more detail below. Furthermore, the use of donor gametes and donor embryos in the

provision of the IVF benefit will be allowed.

3. Additionally, I am issuing this instruction to clarify the impact of the policy changes on the definition of “a service-connected disability that results in the inability of the veteran to procreate without the use of fertility treatment”, found in 38 CFR 17.380, as the current definition does not contemplate the use of donor gametes and donor embryos.

4. I am instructing Department employees to interpret the term “a service-connected disability that results in the inability of the veteran to procreate without the use of fertility treatment” as defined for a female veteran with ovarian function and a patent uterine cavity in 38 CFR 17.380 to also apply to a female veteran without ovarian function or a patent uterine cavity.

Background

5. The National Defense Authorization Act for Fiscal Year 2008, Public Law 110–181, section 1633, 122 Stat. 3, 459 (2008), authorized DoD to provide IVF benefits for certain service members.

6. On April 3, 2012, DoD implemented its IVF policy in a memorandum titled “Policy for Assisted Reproductive Services for the Benefit of Seriously or Severely Ill/Injured (Category II or III) Active Duty Service Members,” accompanied by implementation guidance (collectively referred to throughout this document as the “DoD Policy”).

7. DoD Policy clause IIIA provided:

It is the intent of this policy to provide In vitro (sic) Fertilization (IVF) services only to consenting male members whose injury or illness prevents the successful delivery of their sperm to their spouse's egg and to consenting female members whose injury or illness prevents their egg from being successfully fertilized by their spouse's sperm but who maintain ovarian function and have a patent uterine cavity.

8. DoD Policy clause IIIE provided:

Third-party donation and surrogacy are not covered benefits- the benefit is designed to allow the member and spouse to become biological parents through reproductive technologies where Active Duty injury or illness has made it impossible to conceive naturally.

9. Since 2016, Congress has authorized VA to use medical services funds to provide fertility counseling and treatment, including ART, to certain covered veterans and to the spouses of covered veterans. Public Law 114–223, Division A, Title II, section 260 (Sept. 29, 2016).

10. Congress defined a covered veteran to be one who has a service-connected disability that results in the inability of the veteran to procreate without the use of fertility treatment. *Id.* Congress continued to authorize the use of medical services funds for this purpose in subsequent appropriations laws, most recently in March 2024 in Public Law 118–42, Division A, Title II, section 234.

11. On March 7, 2019, VA published the final rule creating 38 CFR 17.380 implementing Congress's authorization. The regulation provided in pertinent part:

For the purposes of this section, “a service-connected disability that results in the inability of the veteran to procreate without the use of fertility treatment” means, for a male veteran, a service-connected injury or illness that prevents the successful delivery of sperm to an egg; and, for a female veteran with ovarian function and a patent uterine cavity, a service-connected injury or illness that prevents the egg from being successfully fertilized by sperm.

The regulation provides a definition “for a male veteran” and “for a female veteran with ovarian function and a patent uterine cavity”. It does not provide a definition for female veterans without ovarian function and/or without a patent uterine cavity.

12. As a result, female veterans without ovarian function and/or a patent uterine cavity are in an undefined area of eligibility, neither expressly excluded nor expressly included in 38 CFR 17.380. This may inadvertently result in veterans who sustained service-connected disabilities affecting ovarian function and/or the uterine cavity not being considered “covered veterans” for the purposes of fertility benefits.

13. In March 2021, VA issued subregulatory guidance in the form of VHA Directive 1334 to implement its policy for providing IVF counseling and services to eligible veterans and their spouses.

14. VHA Directive 1334, paragraph 1.c., Purpose, notes that DoD Policy governs VA's provisions for IVF counseling and services, and any substantive changes made to DoD's policy will supersede conflicting terms in VHA Directive 1334.

15. On the basis of DoD Policy clauses IIIA and IIIE, VHA Directive 1334 had the effect of limiting VHA to providing IVF services to cisgender opposite-sex legally married couples or other legally married couples with opposite-sex gametes/reproductive organs.

16. On March 8, 2024, DoD Policy was amended. In relevant part, the amendments eliminated the language in

Policy Clause IIIA referred to in paragraph 7, above. The amendment also removed the prohibition on the use of donor gametes in Policy Clause IIIE and expressly allows for the use of donor embryos in the fertility treatment of qualified service members, provided they are obtained at no cost to DoD. Further, the policy was amended to allow a qualified service-member to receive ART services, as clinically appropriate.

Qualifying as a Covered Veteran for Purposes of Receiving IVF Services

17. This Instruction addresses the effect of the DoD Policy amendment on VA's eligibility criteria for veterans and their spouses to receive IVF counseling and services through VHA. The amendment of the DoD Policy supersedes portions of VHA Directive 1334 which were based on the unamended DoD Policy. The amendment also necessitates clarification of the definition of a "service-connected disability that results in the inability of the veteran to procreate without the use of fertility treatment" in 38 CFR 17.380.

18. With the amendment to the DoD Policy, VA IVF benefits will no longer require that a covered Veteran be (1) married,¹ (2) in an opposite-sex relationship, or (3) able to produce their own gametes. Paragraphs 20 through 35 address these changes.

19. Further, lifting the prohibition on donor gametes and donor embryos necessitates clarification of the definition of "a service-connected disability that results in the inability of the veteran to procreate without the use of fertility treatment" found in 38 CFR 17.380. The text of the regulation provides a definition for all male veterans but only provides a definition for a female veteran who has ovarian function and a patent uterine cavity. In that regard, the regulation does not provide a definition for a female veteran who does not have either ovarian function or a patent uterine cavity. The lack of a definition for a female veteran without ovarian function or a patent uterine cavity posed no problem in applying the regulation when there was a prohibition on the use of donated gametes and donated embryos because

¹ VA is only allowed to treat non-veterans when specifically authorized by statute. Public Law 117-328, Division J, Title II, section 234 authorizes VA to provide fertility counseling and identified treatment to "a covered veteran or the spouse of a covered veteran." Therefore, VA will not exclude unmarried veterans from IVF care as discussed throughout, but VA is only authorized to provide IVF care to the non-veteran partner of a veteran if that non-veteran partner is the spouse of the covered veteran.

that prohibition would have prevented such a female veteran from being eligible for IVF services. However, with the lifting of the prohibition on donor gametes and donor embryos, VA must address what the definitional requirements are for a female veteran without ovarian function and/or a patent uterine cavity. Paragraph 35, below, addresses these requirements.

20. VHA Directive 1334, paragraph 2.d., Background, is revised to read:

IVF counseling and services are available to certain seriously injured Veterans no longer able to procreate without the use of fertility treatment. For male Veterans, their service-connected injury or illness must render the Veteran incapable of successfully delivering their sperm to an egg. This definition includes the inability to produce sperm. For female Veterans, with or without ovarian function or a patent uterine cavity, their service-connected injury or illness must render the Veteran incapable of having an egg successfully fertilized by sperm. This definition includes the inability to produce an egg.

21. VHA Directive 1334, paragraph 2.e., Background, is revised to read:

VA may furnish IVF fertility counseling and treatment to Veterans as described herein and their lawful spouses. More specifically, consistent with the Memorandum, VA allows for assisted reproductive services, including evaluations, intrauterine insemination, sperm retrieval, oocyte retrieval, in-vitro fertilization, blastocyst transfer and embryo transfer, to be available to eligible Veterans. VA considers that the cryopreservation of gametes (for both the Veteran and the spouse), not only embryos, is within the scope of available benefits described in the Memorandum. Gamete and embryo cryopreservation and storage are each without limitation on duration until, as explained below, the death of an eligible Veteran. In determining clinical eligibility for IVF services, VA treating providers are to use the same evidence-based clinical eligibility standards outlined in VHA Directive 1332(2), Fertility Evaluation and Treatment.

22. VHA Directive 1334, paragraph 2.f. and g., Background, are struck from the Directive.

23. VHA Directive 1334, paragraph 2.h., Background, is revised to read:

Covered veterans and their spouses may utilize donor gametes and donor embryos obtained at their own expense when receiving IVF counseling and services under this policy. No portion of this benefit will be used to pay for procedures or associated fees for the extraction, storage, or transportation of donor gametes. The creation, storage, and use of resulting embryos are covered by the benefit.

24. VHA Directive 1334, paragraph 2.j., Background, is revised to read:

Although the benefits of cryopreservation and storage of gametes and embryos are not time-limited, these benefits are, practically-

speaking, checked or limited by the death of an eligible Veteran. This is also the practical implication of Clause III.F. of the Memorandum, which requires that VA obtain the separate consent of the Veteran with third party consent being prohibited.

25. VHA Directive 1334, paragraph 2.n., Background, is revised to read:

The Veteran's and spouse's respective eligibility determinations will be made by VHA's Health Eligibility Center. Service-connected conditions covered under this policy include, but are not limited to, poly-trauma, genitourinary injury and spinal cord injury and other anatomical, neurological, infectious and physiological injury and/or illness that are adjudicated by the Veterans Benefits Administration to be service-connected after which VHA IVF program staff will clinically determine if the service-connected condition meets the IVF clinical eligibility criteria *i.e.*, whether the service-connected condition results in loss of procreative ability that cannot be corrected without the use of fertility treatment.

26. VHA Directive 1334, paragraph 3.c., Definitions, is revised to read:

Consent to In Vitro Fertilization. Consent to IVF requires the informed consent of all parties receiving IVF benefits under this policy. Each party must have decision-making capacity to consent to treatment. Consent by a third party, including a proxy decision-maker, is not permitted.

27. VHA Directive 1334, paragraph 3.d., Definitions, is revised to read:

Cryopreservation. Cryopreservation is the freezing of gametes (oocytes or sperm), zygotes (1-cell fertilized oocytes), embryos (typically cryopreserved on day 2, 3, 5, or 6 of development), or gonadal (ovarian or testicular) tissue to allow storage for future use. Cryopreserved sperm can be used for intrauterine insemination (IUI) or IVF after thawing or rewarming. Cryopreserved oocytes require IVF after thawing or rewarming. Cryopreserved tissue may be re-implanted into the body or cultured in vitro after thawing or rewarming. Duration of embryo cryopreservation and storage are without limitation under 38 CFR 17.380 and 17.412 until the death of an eligible Veteran, provided VA continues to have authority to provide these non-limited services.

28. VHA Directive 1334, paragraph 3.j., Definitions, is revised to read:

Infertility. Infertility is a disease, condition, or status characterized by any of the following:

- (1) The inability to achieve a successful pregnancy as established by a patient's medical, sexual, and reproductive history, age, physical findings, diagnostic testing, or any combination of those factors; or
- (2) The need for medical intervention, including, but not limited to, the use of donor gametes or donor embryos in order to achieve a successful pregnancy, either as an individual or with a partner.

29. VHA Directive 1334, paragraph 6. Eligibility Requirements, is revised to read:

To be eligible for fertility services, including IVF, the Veteran must have a service-connected condition that results in the inability to procreate without the use of fertility treatment, as defined above. *NOTE: For additional eligibility information, see appendix A.*

30. VHA Directive 1334, paragraph 7.c.(1), Practices and Procedures, is revised to read:

VA will cover costs of cryopreservation and storage at an independent community laboratory indefinitely up through the end of life of the eligible Veterans. Storage of cryopreserved gametes and embryos will take place at an independent facility in the community, per guidelines outlined in appendix A.

31. VHA Directive 1334, paragraph 7.c.(3), Practices and Procedures, is revised to read:

VA will pay the costs of cryopreservation and storage of cryopreserved oocytes, sperm and embryos indefinitely until the end of the life the eligible Veteran, or until the cryopreserved oocytes, sperm, or embryos are transferred to a third party (for any purpose outside this treatment program).

32. VHA Directive 1334, paragraph 7.e.(1), Practices and Procedures, is struck from the directive.

Gestational surrogacy, as defined in VHA Directive 1334, will remain outside the scope of VA IVF Services. Although the amended DoD Policy allows for a third-party gestational carrier in limited instances, Congress's authorization for VA to provide fertility counseling and treatment, including ART, is limited to providing these services to a covered veteran and the spouse of a covered veteran. Therefore, VA may not provide IVF services to a person who is neither the covered veteran nor the spouse of a covered Veteran.

33. VHA Directive 1334, Appendix A, Eligibility Criteria, is revised to read:

1. To be eligible for In Vitro Fertilization (IVF) under 38 Code of Federal Regulations (CFR) 17.380, a Veteran must have a service-connected disability that results in the Veteran's inability to procreate without the use of fertility treatment.

2. Lawful spouses of eligible Veterans are eligible for fertility counseling and treatment under the program pursuant to 38 CFR 17.412.

34. VHA Directive 1334, Appendix B, In Vitro Fertilization Services, comparison table c is revised to strike:

1. "+ lawful eligible spouses" from the "Eligibility" line;
2. "naturally" from the "Service connection" line;
3. the entirety of the "Marital status" line;

4. the entirety of the "Couples" line;
5. "with opposite-sex gametes" from the "IUI" line;
6. "or an eligible Veteran's lawful divorce" from the "Time limits for cryopreservation of gametes" line;
7. "or an eligible Veteran's lawful divorce" from the "Cryopreservation for embryos" line; and
8. "or an eligible Veteran's lawful divorce" from the "Embryo storage paid by VA" line.

Additionally, the "no" from the "Donate sperm" line is revised to "Allowable but not paid for by VA (Veteran pays for non-Veteran sperm preparation or procedure to non-Veteran)."

35. In 38 CFR 17.380, the term "a service-connected disability that results in the inability of the veteran to procreate without the use of fertility treatment" is interpreted to include:

for a female veteran without ovarian function and/or patent uterine cavity, a service-connected injury or illness that prevents the successful fertilization of an egg by sperm, to include the service-connected loss of ovarian function and/or a patent uterine cavity.

Applicability

36. This Instruction applies to decisions to authorize benefits on or after the date of this Instruction, in which a veteran seeks fertility counseling or IVF services under 38 CFR 17.380 and 17.412.

Signing Authority

Denis McDonough, Secretary of Veterans Affairs, approved and signed this document on March 28, 2024, and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs.

Jeffrey M. Martin,

Assistant Director, Office of Regulation Policy & Management, Office of General Counsel, Department of Veterans Affairs.

[FR Doc. 2024-07040 Filed 4-3-24; 8:45 am]

BILLING CODE 8320-01-P

ENVIRONMENTAL PROTECTION AGENCY

40 CFR Part 52

[EPA-R09-OAR-2023-0599; FRL-11591-02-R9]

Air Plan Approval; Arizona; Maricopa County Air Quality Department

AGENCY: Environmental Protection Agency (EPA).

ACTION: Final rule.

SUMMARY: The Environmental Protection Agency (EPA) is taking final action to approve revisions to the Maricopa County Air Quality Department (MCAQD) portion of the Arizona State Implementation Plan (SIP). These revisions concern a rule that includes definitions for certain terms that are necessary for the implementation of local rules that regulate sources of air pollution. We are approving a local rule under the Clean Air Act (CAA or the Act).

DATES: This rule is effective May 6, 2024.

ADDRESSES: The EPA has established a docket for this action under Docket ID No. EPA-R09-OAR-2023-0599. All documents in the docket are listed on the <https://www.regulations.gov> website. Although listed in the index, some information is not publicly available, e.g., Confidential Business Information (CBI) or other information whose disclosure is restricted by statute. Certain other material, such as copyrighted material, is not placed on the internet and will be publicly available only in hard copy form. Publicly available docket materials are available through <https://www.regulations.gov>, or please contact the person identified in the **FOR FURTHER INFORMATION CONTACT** section for additional availability information. If you need assistance in a language other than English or if you are a person with a disability who needs a reasonable accommodation at no cost to you, please contact the person identified in the **FOR FURTHER INFORMATION CONTACT** section.

FOR FURTHER INFORMATION CONTACT: Kira Wiesinger, EPA Region IX, 75 Hawthorne St., San Francisco, CA 94105; phone: (415) 972-3827; email: wiesinger.kira@epa.gov.

SUPPLEMENTARY INFORMATION:

Throughout this document, "we," "us" and "our" refer to the EPA.

Table of Contents

- I. Proposed Action
- II. Public Comments and EPA Responses
- III. EPA Action
- IV. Incorporation by Reference
- V. Statutory and Executive Order Reviews

I. Proposed Action

On December 27, 2023 (88 FR 89355), the EPA proposed to approve the following rule into the Arizona SIP.

Local agency	Rule #	Rule title	Revised	Submitted
MCAQD	100	General Provisions and Definitions	08/09/2023	08/23/2023

We proposed to approve this rule because we determined that it complies with the relevant CAA requirements. Our proposed action contains more information on the rule and our evaluation.

II. Public Comments and EPA Responses

The EPA’s proposed action provided a 30-day public comment period. During this period, we received no comments on our proposal.

III. EPA Action

No comments were submitted on our proposal. Therefore, as authorized in section 110(k)(3) of the Act, the EPA is approving this rule into the Arizona SIP. The August 9, 2023 version of Rule 100 will replace the previously approved version of this rule in the SIP.

IV. Incorporation by Reference

In this rule, the EPA is finalizing regulatory text that includes incorporation by reference. In accordance with requirements of 1 CFR 51.5, the EPA is finalizing the incorporation by reference of the MCAQD’s Rule 100, “General Provisions and Definitions,” revised on August 9, 2023, which sets forth the legal authority for the Maricopa County Air Pollution Rules and provides definitions of terms used throughout these rules. Therefore, these materials have been approved by the EPA for inclusion in the SIP, have been incorporated by reference by the EPA into that plan, are fully federally enforceable under sections 110 and 113 of the CAA as of the effective date of the final rulemaking of the EPA’s approval, and will be incorporated by reference in the next update to the SIP compilation.¹ The EPA has made, and will continue to make, these documents available through www.regulations.gov and at the EPA Region IX office (please contact the person identified in the **FOR FURTHER INFORMATION CONTACT** section of this preamble for more information).

V. Statutory and Executive Order Reviews

Under the Clean Air Act, the Administrator is required to approve a SIP submission that complies with the provisions of the Act and applicable federal regulations. 42 U.S.C. 7410(k); 40 CFR 52.02(a). Thus, in reviewing SIP

submissions, the EPA’s role is to approve state choices, provided that they meet the criteria of the Clean Air Act. Accordingly, this action merely approves the state law as meeting federal requirements and does not impose additional requirements beyond those imposed by the state law. For that reason, this action:

- Is not a significant regulatory action subject to review by the Office of Management and Budget under Executive Orders 12866 (58 FR 51735, October 4, 1993) and 14094 (88 FR 21879, April 11, 2023);
- Does not impose an information collection burden under the provisions of the Paperwork Reduction Act (44 U.S.C. 3501 *et seq.*);
- Is certified as not having a significant economic impact on a substantial number of small entities under the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*);
- Does not contain any unfunded mandate or significantly or uniquely affect small governments, as described in the Unfunded Mandates Reform Act of 1995 (Pub. L. 104–4);
- Does not have federalism implications as specified in Executive Order 13132 (64 FR 43255, August 10, 1999);
- Is not subject to Executive Order 13045 (62 FR 19885, April 23, 1997) because it approves a state program;
- Is not a significant regulatory action subject to Executive Order 13211 (66 FR 28355, May 22, 2001); and
- Is not subject to requirements of Section 12(d) of the National Technology Transfer and Advancement Act of 1995 (15 U.S.C. 272 note) because application of those requirements would be inconsistent with the Clean Air Act.

In addition, the SIP is not approved to apply on any Indian reservation land or in any other area where the EPA or an Indian tribe has demonstrated that a tribe has jurisdiction. In those areas of Indian country, the rule does not have tribal implications and will not impose substantial direct costs on tribal governments or preempt tribal law as specified by Executive Order 13175 (65 FR 67249, November 9, 2000).

Executive Order 12898 (Federal Actions To Address Environmental Justice in Minority Populations and Low-Income Populations, 59 FR 7629, February 16, 1994) directs Federal agencies to identify and address “disproportionately high and adverse

human health or environmental effects” of their actions on minority populations and low-income populations to the greatest extent practicable and permitted by law. The EPA defines environmental justice (EJ) as “the fair treatment and meaningful involvement of all people regardless of race, color, national origin, or income with respect to the development, implementation, and enforcement of environmental laws, regulations, and policies.” The EPA further defines the term fair treatment to mean that “no group of people should bear a disproportionate burden of environmental harms and risks, including those resulting from the negative environmental consequences of industrial, governmental, and commercial operations or programs and policies.”

The State did not evaluate environmental justice considerations as part of its SIP submittal as the CAA and applicable implementing regulations neither prohibit nor require such an evaluation. The EPA did not perform an EJ analysis and did not consider EJ in this action. Due to the nature of the action being taken here, this action is expected to have a neutral to positive impact on the air quality of the affected area. Consideration of EJ is not required as part of this action, and there is no information in the record inconsistent with the stated goal of Executive Order 12898 of achieving environmental justice for people of color, low-income populations, and Indigenous peoples.

This action is subject to the Congressional Review Act, and the EPA will submit a rule report to each House of the Congress and to the Comptroller General of the United States. This action is not a “major rule” as defined by 5 U.S.C. 804(2).

Under section 307(b)(1) of the Clean Air Act, petitions for judicial review of this action must be filed in the United States Court of Appeals for the appropriate circuit by June 3, 2024. Filing a petition for reconsideration by the Administrator of this final rule does not affect the finality of this action for the purposes of judicial review nor does it extend the time within which a petition for judicial review may be filed, and shall not postpone the effectiveness of such rule or action. This action may not be challenged later in proceedings to enforce its requirements. (See section 307(b)(2).)

¹ 62 FR 27968 (May 22, 1997).

List of Subjects in 40 CFR Part 52

Environmental protection, Air pollution control, Incorporation by reference, Intergovernmental relations, Nitrogen oxides, Ozone, Particulate matter, Reporting and recordkeeping requirements, Volatile organic compounds.

Dated: March 27, 2024.
Martha Guzman Aceves,
Regional Administrator, Region IX.

Part 52, chapter I, title 40 of the Code of Federal Regulations is amended as follows:

PART 52—APPROVAL AND PROMULGATION OF IMPLEMENTATION PLANS

■ 1. The authority citation for Part 52 continues to read as follows:

Authority: 42 U.S.C. 7401 *et seq.*

Subpart D—Arizona

■ 2. In § 52.120, in paragraph (c), amend table 4 by revising the entry for “Rule 100” under the Table headings, “Post-July 1988 Rule Codification” and “Regulation I—General Provisions,” to read as follows:

§ 52.120 Identification of plan.

* * * * *
 (c) * * *

TABLE 4 TO PARAGRAPH (c)—EPA-APPROVED MARICOPA COUNTY AIR POLLUTION CONTROL REGULATIONS

County citation	Title/subject	State effective date	EPA Approval Date	Additional explanation
*	*	*	*	*
Post-July 1988 Rule Codification				
Regulation I—General Provisions				
Rule 100	General Provisions and Definitions	August 9, 2023	[INSERT FIRST PAGE OF FEDERAL REGISTER CITATION], April 4, 2024.	Submitted on August 23, 2023.
*	*	*	*	*

* * * * *
 [FR Doc. 2024-06879 Filed 4-3-24; 8:45 am]
BILLING CODE 6560-50-P

ENVIRONMENTAL PROTECTION AGENCY

40 CFR Part 52

[EPA-R03-OAR-2023-0565; FRL-11415-02-R3]

Air Plan Approval; Pennsylvania; Allegheny County Open Burning Revision and Addition of Mon Valley Air Pollution Episode Requirements

AGENCY: Environmental Protection Agency (EPA).

ACTION: Final rule.

SUMMARY: The Environmental Protection Agency (EPA) is approving a state implementation plan (SIP) revision submitted by the Pennsylvania Department of Environmental Protection (PADEP) on behalf of the Allegheny County Health Department (ACHD). The revision incorporates into the Pennsylvania SIP, particulate matter emission mitigation requirements for industry operating in the portion of Allegheny County known as the “Mon Valley” during weather-related pollution episodes. It also amends a portion of Allegheny County’s open burning regulation, which was previously incorporated into

Pennsylvania’s SIP. EPA is approving this revision to the Allegheny County portion of the Pennsylvania SIP in accordance with the requirements of the Clean Air Act (CAA).

DATES: This final rule is effective on May 6, 2024.

ADDRESSES: EPA has established a docket for this action under Docket ID Number EPA-R03-OAR-2023-0565. All documents in the docket are listed on the www.regulations.gov website. Although listed in the index, some information is not publicly available, e.g., confidential business information (CBI) or other information whose disclosure is restricted by statute. Certain other material, such as copyrighted material, is not placed on the internet and will be publicly available only in hard copy form. Publicly available docket materials are available through www.regulations.gov, or please contact the person identified in the **FOR FURTHER INFORMATION CONTACT** section for additional availability information.

FOR FURTHER INFORMATION CONTACT: Ellen Schmitt, Planning & Implementation Branch (3AD30), Air & Radiation Division, U.S. Environmental Protection Agency, Region III, 1600 John F Kennedy Boulevard, Philadelphia, Pennsylvania 19103. The telephone number is (215) 814-5787. Ms. Schmitt can also be reached via electronic mail at schmitt.ellen@epa.gov.

SUPPLEMENTARY INFORMATION:

I. Background

EPA received a SIP submission from PADEP on August 23, 2023, which EPA subsequently proposed approval of on February 5, 2024 (89 FR 7655). In EPA’s notice of proposed rulemaking (NPRM), EPA proposed to approve changes to ACHD Air Pollution Control Rules and Regulations in Article XXI. This SIP revision includes amendments to section 2105.50 regarding open burning, and adds new section 2106.06, which focuses on mitigating particulate matter air pollution episodes in the Mon Valley.

II. Summary of SIP Revision and EPA Analysis

PADEP’s August 2023 SIP submission seeks to incorporate into Pennsylvania’s SIP a new section (2106.06, Mon Valley Air Pollution Episode) to Allegheny County Article XXI, which focuses on mitigating particulate matter air pollution episodes in the Mon Valley. The SIP submission also seeks to incorporate into the Pennsylvania SIP related changes to Article XXI, section 2105.50, Open Burning.

Article XXI, section 2106.06, Mon Valley Air Episode, is aimed at emission mitigation requirements for industry operating in the portion of the county known as the “Mon Valley” during

weather-related pollution episodes.¹ Section 2106.06 applies to the following sources located within the prescribed Mon Valley Pollution Episode Area: (1) all major and synthetic minor sources of fine particulate matter (PM_{2.5});² (2) all sources that have combined allowable emissions from all emission units of 6.5 tons or more per year of PM_{2.5}; and (3) all sources that have combined allowable emissions from all emission units of 10 tons per year of PM₁₀.³

Section 2106.06 requires applicable sources to submit a mitigation plan to reduce particulate matter emissions for review and approval by ACHD.⁴ Each applicable source's mitigation plan must include a Mon Valley Air Pollution Watch Phase and a Mon Valley Air Pollution Warning Phase, that the source must be prepared for and follow. Each source's mitigation plan must include procedures for when a Mon Valley Air Pollution Watch or Warning is issued. A Mon Valley Air Pollution Watch shall be issued by ACHD if it is "determined from an air quality forecast that for at least the next 24-hour period atmospheric conditions will exist which indicate that the 24-hour average ambient concentration of PM_{2.5} in one or more of the [Mon Valley] municipalities . . . is forecasted to exceed" the value of the 24-hour PM_{2.5} NAAQS of 35

¹ Section 2106.06(d) defines the Mon Valley Air Pollution Episode Area as including the following municipalities: City of Clairton, City of Duquesne, City of McKeesport, Borough of Braddock, Borough of Braddock Hills, Borough of Chalfant, Borough of Dravosburg, Borough of East McKeesport, Borough of East Pittsburgh, Borough of Elizabeth, Borough of Forest Hills, Borough of Glassport, Borough of Jefferson Hills, Borough of Liberty, Borough of Lincoln, Borough of Munhall, Borough of North Braddock, Borough of Port Vue, Borough of Rankin, Borough of Swissvale, Borough of Turtle Creek, Borough of Versailles, Borough of Wall, Borough of West Elizabeth, Borough of West Mifflin, Borough of White Oak, Borough of Wilmerding, Borough of Whitaker, Elizabeth Township, Forward Township, North Versailles Township, and Wilkins Township. See the technical support document (TSD) portion of Pennsylvania's August 23, 2023 Mon Valley Air Pollution Episode SIP submission, section 2.2 Extent of Area, to learn more about how ACHD determined the area of focus within Allegheny County. The SIP submission and incorporated TSD are located in the docket for this proposed rulemaking.

² Definitions of major source and synthetic minor source can be found in ACHD Article XXI, section 2101.20, Definitions.

³ ACHD completed an analysis of the composition of PM_{2.5} in the Mon Valley to determine which sources should be applicable to section 2106.06. It was determined that the majority of excess PM_{2.5} in the Mon Valley is primary in nature and caused by point source emissions from within the area. For additional information, see sections 2.3 and 2.4 of ACHD's TSD which is located in the docket for this proposed rulemaking.

⁴ According to ACHD, as of October 31, 2023, all currently applicable sources have submitted approved mitigation plans.

micrograms per cubic meter (µg/m³).⁵ ACHD shall issue a Mon Valley Air Pollution Warning if during a rolling 24-hour averaging period, an official monitoring station in an applicable municipality exceeds the Mon Valley PM_{2.5} threshold, 35 µg/m³, and ACHD has determined that atmospheric conditions will continue for the next 24-hour period.

To support the reduction of particulate matter pollution during a Mon Valley Air Pollution Watch or Warning, ACHD is also requesting that EPA incorporate into the SIP ACHD's amendment to Article XXI, section 2105.50, Open Burning, which was previously approved into the Commonwealth's SIP.

Other specific requirements of Allegheny County Article XXI section 2106.06 and 2105.50 and the rationale for EPA's action are explained in the NPRM, and will not be restated here.

After review of the August 2023 SIP submission, EPA has determined that the changes to Article XXI are overall SIP strengthening. By incorporating Allegheny County Article XXI section 2106.06 into the Pennsylvania SIP, ACHD adds an additional measure by which the county can help control particulate matter emissions in the Mon Valley, with a relatively quick turn-around time. The amendment to section 2105.50 further supports this measure. This revision will support ACHD's efforts to reduce air pollution emissions in order to minimize the impact on public health.⁶

III. EPA's Response to Comments Received

The public comment period for the NPRM ended on March 6, 2024, and no adverse comments were received. EPA received one comment, which we consider to be vague and non-adverse.

IV. Final Action

For the reasons discussed in detail in the proposed rulemaking and summarized herein, EPA is approving PADEP's August 23, 2023 SIP submission as a revision to the Allegheny County portion of the Pennsylvania SIP.

V. Incorporation by Reference

In this document, EPA is finalizing regulatory text that includes

⁵ Article XXI section 2106.06(c). Article XXI section 2106.06 provides that the "Mon Valley PM_{2.5} threshold level" for purposes of defining a Watch and Warning is the value of the primary 24-hour PM_{2.5} NAAQS.

⁶ Nothing contained in Article XXI section 2106.06 shall impact ACHD's power to issue an Emergency Order pursuant to section 2019.05 of the same Article.

incorporation by reference. In accordance with requirements of 1 CFR 51.5, EPA is finalizing the incorporation by reference of Allegheny County Article XXI section 2106.06 and section 2105.50, as described in section II of this preamble. EPA has made, and will continue to make, these materials generally available through www.regulations.gov and at the EPA Region III Office (please contact the person identified in the **FOR FURTHER INFORMATION CONTACT** section of this preamble for more information). Therefore, these materials have been approved by EPA for inclusion in the SIP, have been incorporated by reference by EPA into that plan, are fully federally enforceable under sections 110 and 113 of the CAA as of the effective date of the final rulemaking of EPA's approval, and will be incorporated by reference in the next update to the SIP compilation.⁷

VI. Statutory and Executive Order Reviews

A. General Requirements

Under the CAA, the Administrator is required to approve a SIP submission that complies with the provisions of the CAA and applicable Federal regulations. 42 U.S.C. 7410(k); 40 CFR 52.02(a). Thus, in reviewing SIP submissions, EPA's role is to approve state choices, provided that they meet the criteria of the CAA. Accordingly, this action merely approves state law as meeting Federal requirements and does not impose additional requirements beyond those imposed by state law. For that reason, this action:

- Is not a significant regulatory action subject to review by the Office of Management and Budget under Executive Orders 12866 (58 FR 51735, October 4, 1993) and 13563 (76 FR 3821, January 21, 2011);
- Does not impose an information collection burden under the provisions of the Paperwork Reduction Act (44 U.S.C. 3501 *et seq.*);
- Is certified as not having a significant economic impact on a substantial number of small entities under the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*);
- Does not contain any unfunded mandate or significantly or uniquely affect small governments, as described in the Unfunded Mandates Reform Act of 1995 (Pub. L. 104-4);
- Does not have federalism implications as specified in Executive Order 13132 (64 FR 43255, August 10, 1999);

⁷ 62 FR 27968 (May 22, 1997).

- Is not an economically significant regulatory action based on health or safety risks subject to Executive Order 13045 (62 FR 19885, April 23, 1997);

- Is not a significant regulatory action subject to Executive Order 13211 (66 FR 28355, May 22, 2001); and

- Is not subject to requirements of Section 12(d) of the National Technology Transfer and Advancement Act of 1995 (15 U.S.C. 272 note) because application of those requirements would be inconsistent with the Clean Air Act;

B. Submission to Congress and the Comptroller General

The Congressional Review Act, 5 U.S.C. 801 *et seq.*, as added by the Small Business Regulatory Enforcement Fairness Act of 1996, generally provides that before a rule may take effect, the agency promulgating the rule must submit a rule report, which includes a copy of the rule, to each House of the Congress and to the Comptroller General of the United States. EPA will submit a report containing this action and other required information to the U.S. Senate, the U.S. House of Representatives, and the Comptroller General of the United States prior to publication of the rule in the **Federal Register**. A major rule cannot take effect until 60 days after it is published in the **Federal Register**. This action is not a “major rule” as defined by 5 U.S.C. 804(2).

C. Petitions for Judicial Review

Under section 307(b)(1) of the CAA, petitions for judicial review of this action must be filed in the United States Court of Appeals for the appropriate circuit by June 3, 2024. Filing a petition for reconsideration by the Administrator of this final rule does not affect the finality of this action for the purposes of judicial review nor does it extend the time within which a petition for judicial review may be filed, and shall not postpone the effectiveness of such rule or action. This action amending

Allegheny County XXI section 2105.50 regarding open burning, and adding new section 2106.06 may not be challenged later in proceedings to enforce its requirements. (See section 307(b)(2).)

D. Environmental Justice

Executive Order 12898 (Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations, 59 FR 7629, February 16, 1994) directs Federal agencies to identify and address “disproportionately high and adverse human health or environmental effects” of their actions on minority populations and low-income populations to the greatest extent practicable and permitted by law. EPA defines environmental justice (E.J.) as “the fair treatment and meaningful involvement of all people regardless of race, color, national origin, or income with respect to the development, implementation, and enforcement of environmental laws, regulations, and policies.” EPA further defines the term fair treatment to mean that “no group of people should bear a disproportionate burden of environmental harms and risks, including those resulting from the negative environmental consequences of industrial, governmental, and commercial operations or programs and policies.”

ACHD did not evaluate environmental justice considerations as part of its SIP submission; the CAA and applicable implementing regulations neither prohibit nor require such an evaluation. EPA did not perform an EJ analysis and did not consider EJ in this final rulemaking. Due to the nature of the action being taken here, this rulemaking is expected to have a neutral to positive impact on the air quality of the affected area. Consideration of EJ is not required as part of this action, and there is no information in the record inconsistent with the stated goal of E.O. 12898 of

achieving environmental justice for people of color, low-income populations, and Indigenous peoples.

In addition, this final rulemaking amending Allegheny County Article XXI section 2105.50 and adding section 2106.06 of Allegheny County Article XXI to Pennsylvania’s SIP, does not have tribal implications as specified by Executive Order 13175 (65 FR 67249, November 9, 2000), because the SIP is not approved to apply in Indian country located in the Commonwealth, and EPA notes that it will not impose substantial direct costs on tribal governments or preempt tribal law.

List of Subjects in 40 CFR Part 52

Environmental protection, Air pollution control, Incorporation by reference, Intergovernmental relations, Particulate matter, Reporting and recordkeeping requirements.

Adam Ortiz,
Regional Administrator, Region III.

For the reasons stated in the preamble, the EPA amends 40 CFR part 52 as follows:

PART 52—APPROVAL AND PROMULGATION OF IMPLEMENTATION PLANS

■ 1. The authority citation for part 52 continues to read as follows:

Authority: 42 U.S.C. 7401 *et seq.*

Subpart NN—Pennsylvania

■ 2. In § 52.2020, the table in paragraph (c)(2) is amended by revising the entry “Open Burning” and by adding the entry “Mon Valley Air Pollution Episode.”

§ 52.2020 Identification of plan.

*	*	*	*	*
(c)	*	*	*	*
(2)	*	*	*	*

Article XX or XXI citation	Title/subject	State effective date	EPA approval date	Additional explanation/ § 52.2063 citation
* 2105.50	* Open Burning	* 11/25/2021	* 4/4/2024, [insert Federal Register citation].	* *
* 2106.06	* Mon Valley Air Pollution Episode	* 11/25/2021	* 4/4/2024, [insert Federal Register citation].	* *
* *	* *	* *	* *	* *

* * * * *

[FR Doc. 2024-06940 Filed 4-3-24; 8:45 am]

BILLING CODE 6560-50-P

ENVIRONMENTAL PROTECTION AGENCY**40 CFR Parts 52, 75, 78, and 97****[EPA-HQ-OAR-2021-0668; FRL-11810-01-OAR]****Partial Denial of Petitions for Reconsideration: Federal “Good Neighbor Plan” for the 2015 Ozone National Ambient Air Quality Standards****AGENCY:** Environmental Protection Agency (EPA).**ACTION:** Notification of action partially denying petitions for reconsideration and administrative stays.

SUMMARY: The Environmental Protection Agency (EPA) is providing notice that it has responded to petitions for reconsideration and administrative stay of a final action under the “good neighbor” or “interstate transport” provision of the Clean Air Act (CAA) published in the **Federal Register** on June 5, 2023, titled “Federal ‘Good Neighbor Plan’ for the 2015 Ozone National Ambient Air Quality Standards” (“Good Neighbor Plan”). In August 2023, the EPA received the four petitions addressed by this action, which seek reconsideration of the Good Neighbor Plan in part on the basis of stays pending judicial review as to certain States issued after the Good Neighbor Plan was promulgated. The EPA is partially denying these four petitions as to this basis. The basis for EPA’s action is set out fully in an enclosure accompanying the response letters, available in the docket for this action. Because the EPA is denying the reconsideration requests, the EPA is also denying associated requests to stay the Good Neighbor Plan filed by two of the four petitioners. At this time, the EPA is not addressing other grounds for reconsideration of the Good Neighbor Plan that have been raised by these or other petitioners.

DATES: April 4, 2024.

FOR FURTHER INFORMATION CONTACT: Mr. Thomas Uher, U.S. Environmental Protection Agency, Office of Air Quality Planning and Standards, Air Quality Policy Division, 109 T.W. Alexander Drive, Mail Code C539-04, Research Triangle Park, NC 27711; phone number: (919) 541-5534; email address: uher.thomas@epa.gov.

SUPPLEMENTARY INFORMATION:**I. Where can I get copies of this document and other related information?**

A copy of this **Federal Register** document, the petitions,¹ the letters denying the four petitions and the accompanying enclosure² describing the full basis for the partial denial of these petitions and associated stay requests, and other materials related to this action are available in the docket that the EPA established for the Good Neighbor Plan rulemaking, under Docket ID No. EPA-HQ-OAR-2021-0668.

All documents in the docket are listed at <https://www.regulations.gov>. Some information may not be publicly available, *i.e.*, Confidential Business Information or other information whose disclosure is restricted by statute. Certain other material, such as copyrighted material, is not placed on the internet and will be publicly available only in hard copy form. Publicly available docket materials are available either electronically at <https://www.regulations.gov> or in hard copy at the U.S. Environmental Protection Agency, EPA Docket Center, William Jefferson Clinton West Building, Room 3334, 1301 Constitution Ave. NW, Washington, DC. The Public Reading Room is open from 8:30 a.m. to 4:30 p.m., Monday through Friday, excluding legal holidays. The telephone number for the Public Reading Room is (202) 566-1744, and the telephone number for the Office of Air and Radiation Docket is (202) 566-1742.

¹ The four petitions are styled respectively as: Petition for Reconsideration and Stay of the Final Rule: Federal “Good Neighbor Plan” for the 2015 Ozone National Ambient Air Quality Standards submitted on behalf of United States Steel Corporation; Petition for Reconsideration and Stay of the Final Rule: Federal “Good Neighbor Plan” for the 2015 Ozone National Ambient Air Quality Standards submitted on behalf of ALLETE, Inc. d/b/a Minnesota Power; Northern States Power Company—Minnesota; Great River Energy; Southern Minnesota Municipal Power Agency; Cleveland-Cliffs, Inc.; and United States Steel Corporation (collectively the “Minnesota Good Neighbor Coalition”); Petition for Reconsideration of the Final Rule for the Promulgation of Air Quality Implementation Plans; State of Arkansas; Federal “Good Neighbor Plan” for the 2015 8-Hour Ozone National Ambient Air Quality Standards submitted on behalf of the Arkansas Department of Energy & Environment, Division of Environmental Quality (DEQ); and Administrative Petition for Reconsideration of the Federal “Good Neighbor Plan” for the 2015 Ozone National Ambient Air Quality Standards submitted on behalf of Hybar LLC.

² See “The EPA’s Basis for Partially Denying Petitions for Reconsideration of the Good Neighbor Plan On Grounds Related to Judicial Stays of the SIP Disapproval Action as to 12 States.”

II. Description of Action

On March 15, 2023, the EPA promulgated the Good Neighbor Plan, which established Federal implementation plan (FIP) requirements for sources in 23 States to address “good neighbor” obligations under CAA section 110(a)(2)(D)(i)(I) for the 2015 ozone NAAQS. Following the finalization and publication of the Good Neighbor Plan, several parties filed petitions with the EPA seeking reconsideration and/or an administrative stay of the Good Neighbor Plan, pursuant to either the Administrative Procedure Act, 5 U.S.C. 705, or CAA Act section 307, 42 U.S.C. 7607. Four of these petitions expressly sought reconsideration by the Agency specifically on grounds related to the issuance of partial judicial stay orders of the separate State implementation plan (SIP) disapproval action (88 FR 9336; Feb. 13, 2023) that had been entered as to several of the States covered by the Good Neighbor Plan.

In the denial letters, the EPA explains that it is partially denying these four petitions for reconsideration, because the objections are not “centrally relevant” to the Good Neighbor Plan in the sense that, having considered the two issues raised in relation to the judicial stays, the EPA found they provide no basis on which the Good Neighbor Plan should be modified or withdrawn. The enclosure to the denial letters articulates the rationale for the EPA’s final response and is available in the docket for this action.

III. Judicial Review

This final action may be challenged in the United States Court of Appeals for the District of Columbia Circuit. Pursuant to CAA section 307(b)(1), petitions for judicial review of this action must be filed in that court within 60 days after the date notice of this final action is published in the **Federal Register**.

CAA section 307(b)(1) governs judicial review of final actions by the EPA. This section provides, in part, that petitions for review must be filed in the D.C. Circuit: (1) when the Agency action consists of “nationally applicable regulations promulgated, or final actions taken, by the Administrator,” or (2) when the Agency action is locally or regionally applicable, if “such action is based on a determination of nationwide scope or effect and if in taking such action the Administrator finds and publishes that such action is based on such a determination.” Numerous petitions for review of the Good Neighbor Plan are currently proceeding

before the D.C. Circuit. For the same reasons that the D.C. Circuit is the appropriate venue for challenges to the Good Neighbor Plan, it is also the appropriate venue for any challenges to this final action.

This action is “nationally applicable” within the meaning of CAA section 307(b)(1) because it denies petitions to reconsider and stay the Good Neighbor Plan, which is itself a nationally applicable action. 88 FR 36654 at 36860; *see also* Order, *Kentucky Energy and Environment Cabinet v. EPA*, No. 23–3605 (6th Cir. Nov. 9, 2023). On its face, the Good Neighbor Plan is nationally applicable because it applies nationally consistent standards and uniform methodologies to 23 States located in ten of the eleven regional Federal judicial circuits across the Nation. 88 FR 36654 at 36860. Although the Good Neighbor Plan is temporarily stayed in 12 States as a result of pending litigation, *see* notes 4 and 5 *supra*, these temporary stays do not alter the rule’s national applicability.³ This denial is likewise nationally applicable because the result of this partial denial of the four petitions identified herein is that the existing Good Neighbor Plan remains in place and undisturbed—and because any judicial order disturbing the EPA’s reasoning herein would impact sources, states, and other parties across multiple judicial circuits.

In the alternative, to the extent a court finds this action or a relevant portion thereof to be locally or regionally applicable, the Administrator hereby makes and publishes a finding that the action is based on several determinations of “nationwide scope or effect” within the meaning of CAA section 307(b)(1). These determinations, which lie at the core of this action and are the primary aspects of the Good Neighbor Plan that petitioners ask the EPA to reconsider, include: the determination that the Good Neighbor Plan is lawful and implementable as applied in any individual state even if it is not in effect for any other particular

State or group of States; the determination that the Good Neighbor Plan is premised on a series of national-scale analyses that are not limited in scope to any particular geography or group of States; and the determination that the Good Neighbor Plan need not be reconsidered as to any group of sources or States on the basis that publication of the Good Neighbor Plan in the **Federal Register** occurred following the issuance of preliminary judicial stay orders as to several States.

Michael S. Regan,
Administrator.

[FR Doc. 2024–06912 Filed 4–3–24; 8:45 am]

BILLING CODE 6560–50–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 2

[WT Docket No. 19–348; DA 24–233; FRS 212104]

Facilitating Shared Use in the 3100–3550 MHz Band; Correction

AGENCY: Federal Communications Commission.

ACTION: Correcting amendment.

SUMMARY: The Federal Communications Commission published a document in the **Federal Register** of March 25, 2024, concerning a non-substantive, editorial revision made by the Wireless Telecommunication Bureau and the Office of Engineering and Technology (WTB/OET) to the Table of Frequency Allocations in the Commission’s Rules (Table 22), which identifies coordinates for Department of Defense Cooperative Planning Areas (CPAs) and Periodic Use Areas (PUAs). The document contained an incorrect instruction regarding the revision to Table 22. This document sets out the correct instruction to amend Table 22.

DATES: Effective April 4, 2024.

FOR FURTHER INFORMATION CONTACT:

Thomas Reed, Wireless Telecommunications Bureau, Mobility Division, (202) 418–0531 or Thomas.reed@fcc.gov. For information

regarding the Paperwork Reduction Act (PRA) information collection requirements, contact Cathy Williams, Office of Managing Director, at 202–418–2918 or cathy.williams@fcc.gov.

SUPPLEMENTARY INFORMATION:

Correction

In the **Federal Register** of March 25, 2024, 89 FR 20548, WTB/OET deleted as redundant, the Norfolk, Virginia Cooperative Planning Area (Norfolk CPA) from the list of CPAs and PUA’s in Table 22, and renamed the Norfolk CPA, the Newport News-Norfolk CPA/PUA. However, the amendment in instruction 2 could not be incorporated as instructed. This document corrects the instruction to amend Table 22.

List of Subjects in 47 CFR Part 2

Administrative practice and procedures, Common carriers, Communications, Communications common carriers, Communications equipment, Disaster assistance, Environmental impact statements, Imports, Radio, Reporting and recordkeeping requirements, Satellites, Telecommunications, Television, Wiretapping and electronic surveillance.

Accordingly, 47 CFR part 2 is corrected by making the following correcting amendment:

PART 2—FREQUENCY ALLOCATIONS AND RADIO TREATY MATTERS; GENERAL RULES AND REGULATIONS

■ 1. The authority citation for part 2 continues to read as follows:

Authority: 47 U.S.C. 154, 302a, 303, and 336, unless otherwise noted.

■ 2. In § 2.106, in paragraph (c)(431), amend table 22 by removing the entry “Norfolk * (includes Fort Story SESEF range)” and adding in its place the entry “Newport News-Norfolk * (includes Fort Story SESEF range)” to read as follows:

§ 2.106 Table of Frequency Allocations.

*	*	*	*	*
(c)	*	*	*	
(431)	*	*	*	

³ Upon the conclusion of the separate supplemental rulemaking, the Good Neighbor Plan may also apply in up to five additional States. *See* 89 FR 12666 (Feb. 24, 2024).

TABLE 22 TO PARAGRAPH (c)(431)—DEPARTMENT OF DEFENSE COOPERATIVE PLANNING AREAS AND PERIODIC USE AREAS

Location name	State	CPA	PUA	Latitude	Longitude	Radius (km)
* * * * *	*	*	*	*	*	*
Newport News-Norfolk* (includes Fort Story SESEF range)	VA	Yes	Yes	36°58'24"	76°26'07"	93
* * * * *	*	*	*	*	*	*

* * * * *

Dated: March 28, 2024.

Amy Brett,
Chief of Staff, Wireless Telecommunications Bureau.

[FR Doc. 2024-07170 Filed 4-3-24; 8:45 am]

BILLING CODE 6712-01-P

Proposed Rules

Federal Register

Vol. 89, No. 66

Thursday, April 4, 2024

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 39

[Docket No. FAA-2024-0994; Project Identifier MCAI-2023-01238-T]

RIN 2120-AA64

Airworthiness Directives; Embraer S.A. (Type Certificate Previously Held by Yaborã Indústria Aeronáutica S.A.; Embraer S.A.) Airplanes

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice of proposed rulemaking (NPRM).

SUMMARY: The FAA proposes to supersede Airworthiness Directive (AD) 2019-24-16, which applies to certain Embraer S.A. Model ERJ 190-100 STD, -100 LR, -100 IGW, and -100 ECJ airplanes; and Model ERJ 190-200 STD, -200 LR, and -200 IGW airplanes. AD 2019-24-16 requires revising the existing maintenance or inspection program, as applicable, to incorporate new or more restrictive airworthiness limitations. Since the FAA issued AD 2019-24-16, the FAA has determined that new or more restrictive airworthiness limitations are necessary. This proposed AD would require revising the existing maintenance or inspection program, as applicable, to incorporate new or more restrictive airworthiness limitations, as specified in an Agência Nacional de Aviação Civil (ANAC) AD, which is proposed for incorporation by reference (IBR). The FAA is proposing this AD to address the unsafe condition on these products.

DATES: The FAA must receive comments on this proposed AD by May 20, 2024.

ADDRESSES: You may send comments, using the procedures found in 14 CFR 11.43 and 11.45, by any of the following methods:

- *Federal eRulemaking Portal:* Go to [regulations.gov](https://www.regulations.gov). Follow the instructions for submitting comments.
- *Fax:* 202-493-2251.

- *Mail:* U.S. Department of Transportation, Docket Operations, M-30, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE, Washington, DC 20590.

- *Hand Delivery:* Deliver to Mail address above between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

AD Docket: You may examine the AD docket at [regulations.gov](https://www.regulations.gov) under Docket No. FAA-2024-0994; or in person at Docket Operations between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The AD docket contains this NPRM, the mandatory continuing airworthiness information (MCAI), any comments received, and other information. The street address for Docket Operations is listed above.

Material Incorporated by Reference:

- For ANAC material that is proposed for IBR in this NPRM, contact National Civil Aviation Agency (ANAC), Aeronautical Products Certification Branch (GGCP), Rua Dr. Orlando Empresarial Aquarius—Torre B—Andares 14 a 18, Parque Residencial Aquarius, CEP 12.246-190—São José dos Campos—SP, Brazil; telephone 55 (12) 3203-6600; email pac@anac.gov.br; website [anac.gov.br/en/](https://www.anac.gov.br/en/). You may find this material on the ANAC website at [sistemas.anac.gov.br/certificacao/DA/DAE.asp](https://www.anac.gov.br/certificacao/DA/DAE.asp).

- For Embraer material identified in this NPRM, contact Embraer S.A., Technical Publications Section (PC 060), Av. Brigadeiro Faria Lima, 2170—Putim—12227-901 São José dos Campos—SP—Brazil; telephone 55 (12) 3927-5852 or 55 (12) 3309-0732; fax 55 (12) 3927-7546; email distrib@embraer.com.br; website www.flyembraer.com.

- You may view this material that is incorporated by reference at the FAA, Airworthiness Products Section, Operational Safety Branch, 2200 South 216th St., Des Moines, WA. For information on the availability of this material at the FAA, call 206-231-3195. It is also available at [regulations.gov](https://www.regulations.gov) under Docket No. FAA-2024-0994.

FOR FURTHER INFORMATION CONTACT: Joshua Bragg, Aviation Safety Engineer, FAA, 1600 Stewart Avenue, Suite 410, Westbury, NY 11590; telephone (216) 316-6418; email joshua.k.bragg@faa.gov.

SUPPLEMENTARY INFORMATION:

Comments Invited

The FAA invites you to send any written relevant data, views, or arguments about this proposal. Send your comments to an address listed under **ADDRESSES**. Include “Docket No. FAA-2024-0994; Project Identifier MCAI-2023-01238-T” at the beginning of your comments. The most helpful comments reference a specific portion of the proposal, explain the reason for any recommended change, and include supporting data. The FAA will consider all comments received by the closing date and may amend this proposal because of those comments.

Except for Confidential Business Information (CBI) as described in the following paragraph, and other information as described in 14 CFR 11.35, the FAA will post all comments received, without change, to [regulations.gov](https://www.regulations.gov), including any personal information you provide. The agency will also post a report summarizing each substantive verbal contact received about this NPRM.

Confidential Business Information

CBI is commercial or financial information that is both customarily and actually treated as private by its owner. Under the Freedom of Information Act (FOIA) (5 U.S.C. 552), CBI is exempt from public disclosure. If your comments responsive to this NPRM contain commercial or financial information that is customarily treated as private, that you actually treat as private, and that is relevant or responsive to this NPRM, it is important that you clearly designate the submitted comments as CBI. Please mark each page of your submission containing CBI as “PROPIN.” The FAA will treat such marked submissions as confidential under the FOIA, and they will not be placed in the public docket of this NPRM. Submissions containing CBI should be sent to Joshua Bragg, Aviation Safety Engineer, FAA, 1600 Stewart Avenue, Suite 410, Westbury, NY 11590; telephone (216) 316-6418; email joshua.k.bragg@faa.gov. Any commentary that the FAA receives that is not specifically designated as CBI will be placed in the public docket for this rulemaking.

Background

The FAA issued AD 2019-24-16, Amendment 39-21005 (84 FR 71772,

December 30, 2019) (AD 2019–24–16), for certain Embraer S.A. Model ERJ 190–100 STD, –100 LR, –100 IGW, and –100 ECJ airplanes; and Model ERJ 190–200 STD, –200 LR, and –200 IGW airplanes. AD 2019–24–16 was prompted by an MCAI originated by ANAC, which is the aviation authority for Brazil. ANAC issued AD 2019–05–02, effective May 2, 2019 (ANAC 2019–05–02) (which corresponds to FAA AD 2019–24–16), to correct an unsafe condition.

AD 2019–24–16 requires revising the existing maintenance or inspection program, as applicable, to incorporate new or more restrictive airworthiness limitations. The FAA issued AD 2019–24–16 to address fatigue cracking of structural components and to address failure of certain system components, which could result in reduced structural integrity and system reliability of the airplane.

Actions Since AD 2019–24–16 Was Issued

Since the FAA issued AD 2019–24–16, ANAC superseded AD 2019–24–16 and issued ANAC AD 2023–12–02, effective December 15, 2023 (ANAC AD 2023–12–02) (also referred to as the MCAI), for certain Embraer S.A. Model ERJ 190–100 STD, –100 LR, –100 IGW, and –100 ECJ airplanes; and Model ERJ 190–200 STD, –200 LR, and –200 IGW airplanes. The MCAI states that new or more restrictive airworthiness limitations have been developed.

The FAA is proposing this AD to address the unsafe condition on these products. You may examine the MCAI in the AD docket at *regulations.gov* under Docket No. FAA–2024–0994.

Related Service Information Under 1 CFR Part 51

The FAA reviewed ANAC AD 2023–12–02. This service information specifies new or more restrictive airworthiness limitations for airplane structures and safe life limits.

This AD also requires the following documents, which the Director of the Federal Register approved for incorporation by reference as of February 3, 2020 (84 FR 71772, December 30, 2019).

- Appendix A—Airworthiness Limitations (AL); to the EMBRAER 190/195 Maintenance Review Board Report, MRB–1928, Revision 12, dated September 27, 2018.
- Appendix A—Airworthiness Limitations (AL), to the EMBRAER Lineage 1000/1000E Maintenance Planning Guide, MPG–2928, Revision 8, dated October 10, 2018.

This material is reasonably available because the interested parties have

access to it through their normal course of business or by the means identified in **ADDRESSES**.

FAA’s Determination

This product has been approved by the aviation authority of another country and is approved for operation in the United States. Pursuant to the FAA’s bilateral agreement with this State of Design Authority, it has notified the FAA of the unsafe condition described in the MCAI referenced above. The FAA is issuing this NPRM after determining that the unsafe condition described previously is likely to exist or develop in other products of the same type design.

Proposed AD Requirements in This NPRM

This proposed AD would retain all requirements of AD 2019–24–16. This proposed AD would also require revising the existing maintenance or inspection program, as applicable, to incorporate additional new or more restrictive airworthiness limitations, which are specified in ANAC AD 2023–12–02 already described, as proposed for incorporation by reference. Any differences with ANAC AD 2023–12–02 are identified as exceptions in the regulatory text of this AD.

This proposed AD would require revisions to certain operator maintenance documents to include new actions (*e.g.*, inspections) and Critical Design Configuration Control Limitations (CDCCLs). Compliance with these actions and CDCCLs is required by 14 CFR 91.403(c). For airplanes that have been previously modified, altered, or repaired in the areas addressed by this proposed AD, the operator may not be able to accomplish the actions described in the revisions. In this situation, to comply with 14 CFR 91.403(c), the operator must request approval for an alternative method of compliance (AMOC) according to paragraph (k)(1) of this proposed AD.

Explanation of Required Compliance Information

In the FAA’s ongoing efforts to improve the efficiency of the AD process, the FAA developed a process to use some civil aviation authority (CAA) ADs as the primary source of information for compliance with requirements for corresponding FAA ADs. The FAA has been coordinating this process with manufacturers and CAAs. As a result, the FAA proposes to incorporate ANAC AD 2023–12–02 by reference in the FAA final rule. This proposed AD would, therefore, require compliance with ANAC AD 2023–12–02

through that incorporation, except for any differences identified as exceptions in the regulatory text of this proposed AD. Service information required by ANAC AD 2023–12–02 for compliance will be available at *regulations.gov* by searching for and locating Docket No. FAA–2024–0994 after the FAA final rule is published.

Airworthiness Limitation ADs Using the New Process

The FAA’s process of incorporating by reference MCAI ADs as the primary source of information for compliance with corresponding FAA ADs has been limited to certain MCAI ADs (primarily those with service bulletins as the primary source of information for accomplishing the actions required by the FAA AD). However, the FAA is now expanding the process to include MCAI ADs that require a change to airworthiness limitation documents, such as airworthiness limitation sections.

For these ADs that incorporate by reference an MCAI AD that changes airworthiness limitations, the FAA requirements are unchanged. Operators must revise the existing maintenance or inspection program, as applicable, to incorporate the information specified in the new airworthiness limitation document. The airworthiness limitations must be followed according to 14 CFR 91.403(c) and 91.409(e).

The previous format of the airworthiness limitation ADs included a paragraph that specified that no alternative actions (*e.g.*, inspections), intervals, or CDCCLs may be used unless the actions, intervals, and CDCCLs are approved as an AMOC in accordance with the procedures specified in the AMOCs paragraph under “Additional AD Provisions.” This new format includes a “New Provisions for Alternative Actions, Intervals, and CDCCLs” paragraph that does not specifically refer to AMOCs, but operators may still request an AMOC to use an alternative action, interval, or CDCCL.

Costs of Compliance

The FAA estimates that this AD, if adopted as proposed, would affect 98 airplanes of U.S. registry. The FAA estimates the following costs to comply with this proposed AD:

The FAA estimates the total cost per operator for the retained actions from AD 2019–24–16 to be \$7,650 (90 work-hours × \$85 per work-hour).

The FAA has determined that revising the existing maintenance or inspection program takes an average of 90 work-hours per operator, although the agency

recognizes that this number may vary from operator to operator. Since operators incorporate maintenance or inspection program changes for their affected fleet(s), the FAA has determined that a per-operator estimate is more accurate than a per-airplane estimate.

The FAA estimates the total cost per operator for the new proposed actions to be \$7,650 (90 work-hours × \$85 per work-hour).

Authority for This Rulemaking

Title 49 of the United States Code specifies the FAA's authority to issue rules on aviation safety. Subtitle I, section 106, describes the authority of the FAA Administrator. Subtitle VII: Aviation Programs, describes in more detail the scope of the Agency's authority.

The FAA is issuing this rulemaking under the authority described in Subtitle VII, Part A, Subpart III, Section 44701: General requirements. Under that section, Congress charges the FAA with promoting safe flight of civil aircraft in air commerce by prescribing regulations for practices, methods, and procedures the Administrator finds necessary for safety in air commerce. This regulation is within the scope of that authority because it addresses an unsafe condition that is likely to exist or develop on products identified in this rulemaking action.

Regulatory Findings

The FAA determined that this proposed AD would not have federalism implications under Executive Order 13132. This proposed AD would not have a substantial direct effect on the States, on the relationship between the national Government and the States, or on the distribution of power and responsibilities among the various levels of government.

For the reasons discussed above, I certify this proposed regulation:

(1) Is not a "significant regulatory action" under Executive Order 12866,

(2) Would not affect intrastate aviation in Alaska, and

(3) Would not have a significant economic impact, positive or negative, on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

List of Subjects in 14 CFR Part 39

Air transportation, Aircraft, Aviation safety, Incorporation by reference, Safety.

The Proposed Amendment

Accordingly, under the authority delegated to me by the Administrator,

the FAA proposes to amend 14 CFR part 39 as follows:

PART 39—AIRWORTHINESS DIRECTIVES

■ 1. The authority citation for part 39 continues to read as follows:

Authority: 49 U.S.C. 106(g), 40113, 44701.

§ 39.13 [Amended]

■ 2. The FAA amends § 39.13 by:

■ a. Removing Airworthiness Directive (AD) 2019–24–16, Amendment 39–21005 (84 FR 71772, December 30, 2019); and

■ b. Adding the following new AD:

Embraer S.A. (Type Certificate Previously Held by Yaborã Indústria Aeronáutica S.A.; Embraer S.A.; Empresa Brasileira de Aeronáutica S.A. (EMBRAER)); Docket No. FAA–2024–0994; Project Identifier MCAI–2023–01238–T.

(a) Comments Due Date

The FAA must receive comments on this airworthiness directive (AD) by May 20, 2024.

(b) Affected ADs

This AD replaces AD 2019–24–16, Amendment 39–21005 (84 FR 71772, December 30, 2019) (AD 2019–24–16).

(c) Applicability

This AD applies to Embraer S.A. Model ERJ 190–100 STD, –100 LR, –100 ECJ, and –100 IGW airplanes; and Model ERJ 190–200 STD, –200 LR, and –200 IGW airplanes; certificated in any category; as identified in Agência Nacional de Aviação Civil (ANAC) AD 2023–12–02, effective December 15, 2023 (ANAC AD 2023–12–02).

(d) Subject

Air Transport Association (ATA) of America Code 05, Time Limits/Maintenance Checks.

(e) Unsafe Condition

This AD was prompted by a determination that new or more restrictive airworthiness limitations are necessary. The FAA is issuing this AD to address failure of certain system components. The unsafe condition, if not addressed, could result in reduced structural integrity and system reliability of the airplane.

(f) Compliance

Comply with this AD within the compliance times specified, unless already done.

(g) Retained Revision of the Existing Maintenance or Inspection Program, With No Changes

This paragraph restates the requirements of paragraph (i) of AD 2019–24–16, with no changes. For airplanes having serial numbers 19000002, 19000004, 19000006 through 19000213 inclusive, 19000215 through 19000276 inclusive, 19000278 through 19000466 inclusive, 19000468 through 19000525 inclusive, and 19000527 through

19000758 inclusive: Do the revision required by paragraph (g)(1) or (2) of this AD, as applicable. Accomplishing the revision of the existing maintenance or inspection program required by paragraph (i) of this AD terminates the requirements of this paragraph.

(1) For Model ERJ 190–100 STD, ERJ 190–100 LR, ERJ 190–100 IGW, ERJ 190–200 STD, ERJ 190–200 LR, and ERJ 190–200 IGW airplanes: Within 90 days after February 3, 2020 (the effective date of AD 2019–24–16), revise the existing maintenance or inspection program, as applicable, to incorporate the information specified in Appendix A—Airworthiness Limitations (AL); to the EMBRAER 190/195 Maintenance Review Board Report, MRB–1928, Revision 12, dated September 27, 2018 (“EMBRAER 190/195 MRB–1928, Revision 12”). The initial compliance times for doing the tasks are at the later of the times specified in paragraphs (g)(1)(i) and (ii) of this AD.

(i) Within the applicable times specified in EMBRAER 190/195 MRB–1928, Revision 12. For the purposes of this AD, the initial compliance times (identified as “Threshold” or “T” in EMBRAER 190/195 MRB–1928, Revision 12) are expressed in “total flight cycles or “total flight hours” as applicable.

(ii) Within 90 days or 600 flight cycles after February 3, 2020 (the effective date of AD 2019–24–16), whichever occurs later.

(2) For Model ERJ 190–100 ECJ airplanes: Within 90 days after February 3, 2020 (the effective date of AD 2019–24–16), revise the existing maintenance or inspection program, as applicable, to incorporate the tasks specified in Appendix A—Airworthiness Limitations (AL), to the EMBRAER Lineage 1000/1000E Maintenance Planning Guide, MPG–2928, Revision 8, dated October 10, 2018 (“EMBRAER Lineage 1000/1000E MPG–2928, Revision 8”). The initial compliance times for the tasks are at the later of the times specified in paragraphs (g)(2)(i) and (ii) of this AD.

(i) Within the applicable times specified in EMBRAER Lineage 1000/1000E MPG–2928, Revision 8. For the purposes of this AD, the initial compliance times (identified as “Threshold” or “T” in EMBRAER Lineage 1000/1000E MPG–2928, Revision 8) are expressed in “total flight cycles” or “total flight hours” as applicable.

(ii) Within 90 days or 600 flight cycles after February 3, 2020 (the effective date of AD 2019–24–16), whichever occurs later.

(h) Retained Restrictions on Alternative Actions, Intervals, and Critical Design Configuration Control Limitations (CDCCLs), With a New Exception

This paragraph restates the requirements of paragraph (j) of AD 2019–24–16, with a new exception. Except as required by paragraph (i) of this AD: After the existing maintenance or inspection program has been revised as required by paragraph (g) of this AD, no alternative actions (e.g., inspections), intervals, or CDCCLs may be used unless the actions, intervals, and CDCCLs are approved as an AMOC in accordance with the procedures specified in paragraph (k)(1) of this AD.

(i) New Revision of the Existing Maintenance or Inspection Program

Except as specified in paragraph (j) of this AD: Comply with all required actions and compliance times specified in, and in accordance with, ANAC AD 2023–12–02. Accomplishing the revision of the existing maintenance or inspection program required by this paragraph terminates the requirements of paragraph (g) of this AD.

(j) Exceptions to ANAC AD 2023–12–02

(1) Where ANAC AD 2023–12–02 refers to its effective date, this AD requires using the effective date of this AD.

(2) This AD does not adopt paragraph (d) of ANAC AD 2023–12–02.

(3) Where paragraph (c) of ANAC AD 2023–12–02 refers to “alternative inspections or inspection intervals,” for this AD, replace that text with “alternative actions (e.g., inspections), intervals, and CDCCLs.”

(k) Additional AD Provisions

The following provisions also apply to this AD:

(1) *Alternative Methods of Compliance (AMOCs)*: The Manager, International Validation Branch, FAA, has the authority to approve AMOCs for this AD, if requested using the procedures found in 14 CFR 39.19. In accordance with 14 CFR 39.19, send your request to your principal inspector or responsible Flight Standards Office, as appropriate. If sending information directly to the manager of the International Validation Branch, mail it to the address identified in paragraph (l) of this AD. Information may be emailed to: 9-AVS-AIR-730-AMOC@faa.gov.

Before using any approved AMOC, notify your appropriate principal inspector, or lacking a principal inspector, the manager of the responsible Flight Standards Office.

(2) *Contacting the Manufacturer*: For any requirement in this AD to obtain instructions from a manufacturer, the instructions must be accomplished using a method approved by the Manager, International Validation Branch, FAA; or ANAC; or ANAC’s authorized Designee. If approved by the ANAC Designee, the approval must include the Designee’s authorized signature.

(l) Additional Information

For more information about this AD, contact Joshua Bragg, Aviation Safety Engineer, FAA, 1600 Stewart Avenue, Suite 410, Westbury, NY 11590; telephone (216) 316–6418; email joshua.k.bragg@faa.gov.

(m) Material Incorporated by Reference

(1) The Director of the Federal Register approved the incorporation by reference (IBR) of the service information listed in this paragraph under 5 U.S.C. 552(a) and 1 CFR part 51.

(2) You must use this service information as applicable to do the actions required by this AD, unless this AD specifies otherwise.

(3) The following service information was approved for IBR on [DATE 35 DAYS AFTER PUBLICATION OF THE FINAL RULE].

(i) Agência Nacional de Aviação Civil (ANAC) AD 2023–12–02, effective December 15, 2023.

(ii) [Reserved]

(4) The following service information was approved for IBR on February 3, 2020 (84 FR 71772, December 30, 2019).

(i) Appendix A—Airworthiness Limitations (AL); to the EMBRAER 190/195 Maintenance Review Board Report, MRB–1928, Revision 12, dated September 27, 2018.

(ii) Appendix A—Airworthiness Limitations (AL), to the EMBRAER Lineage 1000/1000E Maintenance Planning Guide, MPG–2928, Revision 8, dated October 10, 2018.

(5) For ANAC AD 2023–12–02, contact ANAC, Aeronautical Products Certification Branch (GGCP), Rua Dr. Orlando Feirabend Filho, 230—Centro Empresarial Aquarius—Torre B—Andares 14 a 18, Parque Residencial Aquarius, CEP 12.246–190—São José dos Campos—SP, Brazil; telephone 55 (12) 3203–6600; email pac@anac.gov.br; website anac.gov.br/en/. You may find this ANAC AD on the ANAC website at sistemas.anac.gov.br/certificacao/DA/DAE.asp.

(6) For Embraer material identified in this AD, contact Embraer S.A., Technical Publications Section (PC 060), Av. Brigadeiro Faria Lima, 2170—Putim—12227–901 São José dos Campos—SP—Brazil; telephone 55 (12) 3927–5852 or 55 (12) 3309–0732; fax 55 (12) 3927–7546; email distrib@embraer.com.br; website www.flyembraer.com.

(7) You may view this material that is incorporated by reference at the FAA, Airworthiness Products Section, Operational Safety Branch, 2200 South 216th St., Des Moines, WA. For information on the availability of this material at the FAA, call 206–231–3195.

(8) You may view this material at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, visit www.archives.gov/federal-register/cfr/ibr-locations, or email fr.inspection@nara.gov.

Issued on March 28, 2024.

Victor Wicklund,

Deputy Director, Compliance & Airworthiness Division, Aircraft Certification Service.

[FR Doc. 2024–07033 Filed 4–3–24; 8:45 am]

BILLING CODE 4910–13–P

DEPARTMENT OF TRANSPORTATION**Federal Aviation Administration****14 CFR Part 71**

[Docket No. FAA–2024–0367; Airspace Docket No. 23–ASO–41]

RIN 2120–AA66

Amendment of United States Area Navigation (RNAV) Route Q–83; Eastern United States

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice of proposed rulemaking (NPRM).

SUMMARY: This action proposes to amend United States Area Navigation (RNAV) Route Q–83 in the eastern United States. This action supports the Northeast Corridor Atlantic Coast Routes (NEC ACR) Optimization Project to improve the efficiency of the National Airspace System (NAS).

DATES: Comments must be received on or before May 20, 2024.

ADDRESSES: Send comments identified by FAA Docket No. FAA–2024–0367 and Airspace Docket No. 23–ASO–41 using any of the following methods:

* *Federal eRulemaking Portal:* Go to www.regulations.gov and follow the online instructions for sending your comments electronically.

* *Mail:* Send comments to Docket Operations, M–30; U.S. Department of Transportation, 1200 New Jersey Avenue SE, Room W12–140, West Building Ground Floor, Washington, DC 20590–0001.

* *Hand Delivery or Courier:* Take comments to Docket Operations in Room W12–140 of the West Building Ground Floor at 1200 New Jersey Avenue SE, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

* *Fax:* Fax comments to Docket Operations at (202) 493–2251.

Docket: Background documents or comments received may be read at www.regulations.gov at any time. Follow the online instructions for accessing the docket or go to the Docket Operations in Room W12–140 of the West Building Ground Floor at 1200 New Jersey Avenue SE, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

FAA Order JO 7400.11H, Airspace Designations and Reporting Points, and subsequent amendments can be viewed online at www.faa.gov/air_traffic/publications/. You may also contact the Rules and Regulations Group, Office of Policy, Federal Aviation Administration, 800 Independence Avenue SW, Washington, DC 20591; telephone: (202) 267–8783.

FOR FURTHER INFORMATION CONTACT:

Brian Vidis, Rules and Regulations Group, Office of Policy, Federal Aviation Administration, 800 Independence Avenue SW, Washington, DC 20591; telephone: (202) 267–8783.

SUPPLEMENTARY INFORMATION:**Authority for This Rulemaking**

The FAA’s authority to issue rules regarding aviation safety is found in Title 49 of the United States Code. Subtitle I, Section 106 describes the authority of the FAA Administrator. Subtitle VII, Aviation Programs,

describes in more detail the scope of the agency's authority. This rulemaking is promulgated under the authority described in Subtitle VII, Part A, Subpart I, Section 40103. Under that section, the FAA is charged with prescribing regulations to assign the use of the airspace necessary to ensure the safety of aircraft and the efficient use of airspace. This regulation is within the scope of that authority as it amends the route structure to maintain the efficient flow of air traffic within the NAS.

Comments Invited

The FAA invites interested persons to participate in this rulemaking by submitting written comments, data, or views. Comments are specifically invited on the overall regulatory, aeronautical, economic, environmental, and energy-related aspects of the proposal. The most helpful comments reference a specific portion of the proposal, explain the reason for any recommended change, and include supporting data. To ensure the docket does not contain duplicate comments, commenters should submit only one time if comments are filed electronically, or commenters should send only one copy of written comments if comments are filed in writing.

The FAA will file in the docket all comments it receives, as well as a report summarizing each substantive public contact with FAA personnel concerning this proposed rulemaking. Before acting on this proposal, the FAA will consider all comments it receives on or before the closing date for comments. The FAA will consider comments filed after the comment period has closed if it is possible to do so without incurring expense or delay. The FAA may change this proposal in light of the comments it receives.

Privacy: In accordance with 5 U.S.C. 553(c), DOT solicits comments from the public to better inform its rulemaking process. DOT posts these comments, without edit, including any personal information the commenter provides, to www.regulations.gov, as described in the system of records notice (DOT/ALL-14 FDMS), which can be reviewed at www.dot.gov/privacy.

Availability of Rulemaking Documents

An electronic copy of this document may be downloaded through the internet at www.regulations.gov. Recently published rulemaking documents can also be accessed through the FAA's web page at www.faa.gov/air_traffic/publications/airspace_amendments/.

You may review the public docket containing the proposal, any comments received and any final disposition in person in the Dockets Operations office (see **ADDRESSES** section for address, phone number, and hours of operations). An informal docket may also be examined during normal business hours at the office of the Eastern Service Center, Federal Aviation Administration, Room 210, 1701 Columbia Avenue, College Park, GA, 30337.

Incorporation by Reference

United States Area Navigation Routes (Q-Routes) are published in paragraph 2006 of FAA Order JO 7400.11, Airspace Designations and Reporting Points, which is incorporated by reference in 14 CFR 71.1 on an annual basis. This document proposes to amend the current version of that order, FAA Order JO 7400.11H, dated August 11, 2023, and effective September 15, 2023. These updates would be published in the next update to FAA Order JO 7400.11. That order is publicly available as listed in the **ADDRESSES** section of this document.

FAA Order JO 7400.11H lists Class A, B, C, D, and E airspace areas, air traffic service routes, and reporting points.

The Proposal

The FAA is proposing an amendment to 14 CFR part 71 to amend RNAV Route Q-83 in the eastern United States. This action supports the NEC ACR Optimization Project to improve the efficiency of the NAS. The proposed route changes are described below.

Q-83: Q-83 currently extends between the JEVED, GA, Waypoint (WP) and the SLOJO, SC, WP. The FAA proposes to remove the SLOJO WP from the route and extend Q-83 to the north between the EFFAY, SC, WP and the Greensboro, NC (GSO), Very High Frequency Omnidirectional Range/Tactical Air Navigation (VORTAC). The proposed RNAV route extension would provide more efficient routing for aircraft transitioning between Jacksonville Air Route Traffic Control Center (ARTCC) and Atlanta ARTCC, as the Greensboro VORTAC is located on the boundary between Jacksonville ARTCC and Atlanta ARTCC.

Additionally, the TAALN, GA, WP and the KONEY, SC, WP are removed from the route's legal description as they make up segments that contain a turn of less than one degree. As amended, the route would be changed to extend between the JEVED WP and the Greensboro VORTAC.

Regulatory Notices and Analyses

The FAA has determined that this proposed regulation only involves an established body of technical regulations for which frequent and routine amendments are necessary to keep them operationally current. It, therefore: (1) is not a "significant regulatory action" under Executive Order 12866; (2) is not a "significant rule" under DOT Regulatory Policies and Procedures (44 FR 11034; February 26, 1979); and (3) does not warrant preparation of a regulatory evaluation as the anticipated impact is so minimal. Since this is a routine matter that will only affect air traffic procedures and air navigation, it is certified that this proposed rule, when promulgated, will not have a significant economic impact on a substantial number of small entities under the criteria of the Regulatory Flexibility Act.

Environmental Review

This proposal will be subject to an environmental analysis in accordance with FAA Order 1050.1F, "Environmental Impacts: Policies and Procedures" prior to any FAA final regulatory action.

List of Subjects in 14 CFR Part 71

Airspace, Incorporation by reference, Navigation (air).

The Proposed Amendment

In consideration of the foregoing, the Federal Aviation Administration proposes to amend 14 CFR part 71 as follows:

PART 71—DESIGNATION OF CLASS A, B, C, D, AND E AIRSPACE AREAS; AIR TRAFFIC SERVICE ROUTES; AND REPORTING POINTS

■ 1. The authority citation for 14 CFR part 71 continues to read as follows:

Authority: 49 U.S.C. 106(f), 106(g); 40103, 40113, 40120; E.O. 10854, 24 FR 9565, 3 CFR, 1959–1963 Comp., p. 389.

§ 71.1 [Amended]

■ 2. The incorporation by reference in 14 CFR 71.1 of FAA Order JO 7400.11H, Airspace Designations and Reporting Points, dated August 11, 2023, and effective September 15, 2023, is amended as follows:

Paragraph 2006 United States Area Navigation Routes.

* * * * *

Q-83 JEVED, GA to Greensboro, NC (GSO) [Amended]

JEVED, GA	WP	(Lat. 31°15'02.60" N, long. 081°03'40.14" W)
ROYCO, GA	WP	(Lat. 31°35'10.38" N, long. 081°02'22.45" W)
WURFL, SC	WP	(Lat. 32°31'46.59" N, long. 081°01'08.07" W)
EFFAY, SC	WP	(Lat. 34°15'30.67" N, long. 080°30'37.94" W)
Greensboro, NC (GSO)	VORTAC	(Lat. 36°02'44.50" N, long. 079°58'34.94" W)

* * * * *

Issued in Washington, DC, on March 29, 2024.

Frank Lias,

Manager, Rules and Regulations Group.

[FR Doc. 2024-07085 Filed 4-3-24; 8:45 am]

BILLING CODE 4910-13-P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

50 CFR Part 17

[Docket No. FWS-R8-ES-2023-0092;
FXES1111090FEDR-245-FF09E21000]

RIN 1018-BH08

Endangered and Threatened Wildlife and Plants; Threatened Species Status With Section 4(d) Rule for the Northwestern Pond Turtle and Southwestern Pond Turtle

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Proposed rule; reopening of comment period.

SUMMARY: We, the U.S. Fish and Wildlife Service (Service), are reopening the public comment period on our October 3, 2023, proposed rule to list the northwestern pond turtle (*Actinemys marmorata*), a species from Washington, Oregon, Nevada, and northern and central California, and the southwestern pond turtle (*Actinemys pallida*), a species from central and southern California and Baja California, Mexico, as threatened species under the Endangered Species Act of 1973, as amended (Act). We are taking this action to allow all interested parties an additional opportunity to comment on the proposed listing of the two species and the proposed rule issued under section 4(d) of the Act ("4(d) rule") for the species. Comments previously submitted need not be resubmitted and will be fully considered in our final determinations.

DATES: The comment period on the proposed rule that published October 3, 2023 (88 FR 68370), is reopened. We will accept comments received or postmarked on or before May 6, 2024. Please note that comments submitted electronically using the Federal eRulemaking Portal (see **ADDRESSES**,

below) must be received by 11:59 p.m. eastern time on the closing date to ensure consideration.

ADDRESSES: *Availability of documents:* You may obtain copies of the October 3, 2023, proposed rule and associated documents on the internet at <https://www.regulations.gov> under Docket No. FWS-R8-ES-2023-0092.

Written comments: You may submit comments by one of the following methods:

(1) *Electronically:* Go to the Federal eRulemaking Portal: <https://www.regulations.gov>. In the Search box, enter FWS-R8-ES-2023-0092, which is the docket number for the proposed rule. Then, click on the Search button. On the resulting page, in the panel on the left side of the screen, under the Document Type heading, check the Proposed Rule box to locate this document. You may submit a comment by clicking on "Comment."

(2) *By hard copy:* Submit by U.S. mail to: Public Comments Processing, Attn: FWS-R8-ES-2023-0092, U.S. Fish and Wildlife Service, MS: PRB/3W, 5275 Leesburg Pike, Falls Church, VA 22041-3803.

We request that you send comments only by the methods described above. We will post all comments on <https://www.regulations.gov>. This generally means that we will post any personal information you provide us (see Public Comments, below, for more information).

FOR FURTHER INFORMATION CONTACT: Steve Henry, Field Supervisor, U.S. Fish and Wildlife Service, 2493 Portola Road, Suite B, Ventura, CA 93003; telephone 805-644-1766. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States. Please see Docket No. FWS-R8-ES-2023-0092 on <https://www.regulations.gov> for a document that summarizes the October 3, 2023, proposed rule.

SUPPLEMENTARY INFORMATION:

Background

On October 3, 2023, we published a proposed rule (88 FR 68370) to list the northwestern and southwestern pond turtles as threatened species with a 4(d) rule under the Act (16 U.S.C. 1531 *et seq.*). The proposed rule opened a 60-day public comment period, ending December 4, 2023. We are reopening the comment period to allow the public an additional opportunity to provide comments on the October 3, 2023, proposed rule.

For a description of previous Federal actions concerning listing of the northwestern and southwestern pond turtle and information on the types of comments that would be helpful to us in promulgating this rulemaking action, please refer to the October 3, 2023, proposed rule (88 FR 68370 at 68371-68372).

Public Comments

If you submit information via <https://www.regulations.gov>, your entire submission—including your personal identifying information—will be posted on the website. If your submission is made via a hardcopy that includes personal identifying information, you may request at the top of your document that we withhold this information from public review. However, we cannot guarantee that we will be able to do so. We will post all hardcopy submissions on <https://www.regulations.gov>.

Comments and materials we receive, as well as supporting documentation we used in preparing the October 3, 2023, proposed rule, will be available for public inspection on <https://www.regulations.gov> at Docket No. FWS-R8-ES-2023-0092.

Authors

The primary authors of this document are the staff members of the Fish and Wildlife Service's Species Assessment Team and the Ventura Fish and Wildlife Office.

Authority

The authority for this action is the Endangered Species Act of 1973, as amended (16 U.S.C. 1531 *et seq.*).

Martha Williams,

Director, U.S. Fish and Wildlife Service.

[FR Doc. 2024-07094 Filed 4-3-24; 8:45 am]

BILLING CODE 4333-15-P

DEPARTMENT OF COMMERCE**National Oceanic and Atmospheric Administration****50 CFR Parts 679**

RIN 0648–BM69

Fisheries of the Exclusive Economic Zone off Alaska; Amendment 113 to the Fishery Management Plan for the Groundfish of the Gulf of Alaska; Central Gulf of Alaska Rockfish Program Adjustments

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of availability of fishery management plan amendment; request for comments.

SUMMARY: The North Pacific Fishery Management Council (Council) submitted to the Secretary of Commerce for review, Amendment 113 to the Fishery Management Plan (FMP) for the Groundfish of the Gulf of Alaska (GOA). If approved, Amendment 113 would modify specific provisions of the Central Gulf of Alaska (CGOA) Rockfish Program (RP) to change the season start date, remove the catcher vessel (CV) cooperative holding cap, and revise the processing and harvesting caps implemented in the RP. This action is necessary to provide increased flexibility and efficiency, and better ensure the rockfish species total allowable catch (TAC) is fully harvested and landed in Kodiak while still maintaining the intent of the RP. Amendment 113 is intended to promote the goals and objectives of the Magnuson-Stevens Fishery Conservation and Management Act (Magnuson-Stevens Act), the FMP, and other applicable laws.

DATES: Comments must be received no later than June 3, 2024.

ADDRESSES: You may submit comments on this document, identified by NOAA–NMFS–2023–0149 by any of the following methods:

- *Electronic Submission:* Submit all electronic public comments via the Federal e-Rulemaking Portal. Go to <https://www.regulations.gov> and enter NOAA–NMFS–2023–0149 in the Search box (note: copying and pasting the FDMS Docket Number directly from this document may not yield search results). Click on the “Comment” icon, complete the required fields, and enter or attach your comments.

- *Mail:* Submit written comments to Gretchen Harrington, Assistant Regional

Administrator, Sustainable Fisheries Division, Alaska Region NMFS. Mail comments to P.O. Box 21668, Juneau, AK 99802–1668.

Instructions: Comments sent by any other method, to any other address or individual, or received after the end of the comment period, may not be considered by NMFS. All comments received are a part of the public record and will generally be posted for public viewing on <https://www.regulations.gov> without change. All personal identifying information (e.g., name, address, etc.), confidential business information, or otherwise sensitive information submitted voluntarily by the sender will be publicly accessible. NMFS will accept anonymous comments (enter “N/A” in the required fields if you wish to remain anonymous).

Electronic copies of Amendment 113 to the FMP, the Environmental Assessment/Regulatory Impact Review prepared for this action (the Analysis), and the Finding of No Significant Impact prepared for this action may be obtained from www.regulations.gov and the NMFS Alaska Region website at <https://www.fisheries.noaa.gov/region/alaska>.

Written comments regarding the burden-hour estimates or other aspects of the collection-of-information requirements contained in this proposed rule may be submitted to NMFS at the above address and to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting “Currently under Review—Open for Public Comments” or by using the search function.

FOR FURTHER INFORMATION CONTACT: Joel Kraski, 907–586–7228 or joel.kraski@noaa.gov.

SUPPLEMENTARY INFORMATION: The Council submitted Amendment 113 to the FMP to the Secretary for review. If approved by the Secretary, Amendment 113 would provide increased flexibility, efficiency and add protection against unforeseen circumstances for the fishery by expanding the fishing season to harvest and land CGOA rockfish TAC in Kodiak as intended, while still maintaining the intent of the RP. Amendment 113 is intended to promote the goals and objectives of the Magnuson-Stevens Act, the FMP, and other applicable laws.

The Magnuson-Stevens Act requires that each regional fishery management council submit any fishery management plan amendment it prepares to NMFS for review and approval, disapproval, or partial approval by the Secretary. The Magnuson-Stevens Act also requires that NMFS, upon receiving a fishery

management plan amendment, immediately publish a document in the **Federal Register** announcing that the amendment is available for public review and comment. This document announces that proposed Amendment 113 to the FMP is available for public review and comment.

The Council prepared, and the Secretary approved, the GOA FMP under the authority of section 302(h)(1) and 303(b) of the Magnuson-Stevens Act, 16 U.S.C. 1801 *et seq.* The FMP is implemented by Federal regulations governing U.S. fisheries at 50 CFR part 679. The Council is authorized to prepare and recommend a GOA FMP amendment for the conservation and management of a fishery covered under the GOA FMP.

The RP provides exclusive harvesting privileges for vessels using trawl gear to harvest a specific set of rockfish species and associated species incidentally harvested to those rockfish in the Central GOA, an area from 147° W long. to 159° W long. The granting of exclusive harvesting is commonly called rationalization. The rockfish primary species rationalized under the RP are northern rockfish, Pacific ocean perch, and dusky rockfish. The incidentally harvested groundfish taken in the primary rockfish fisheries and which also are rationalized under the RP are called the secondary species. The secondary species include Pacific cod, roughey rockfish, shortraker rockfish, and sablefish. In addition to these secondary species, the RP allocates a portion of the halibut bycatch mortality limit annually specified for the GOA trawl fisheries to RP participants. The Council included the port delivery requirement to address industry concern that harvesters participating in the RP continue to deliver catch to the traditional port of Kodiak (76 FR 81248, December 27, 2011).

Use caps, or caps, are the maximum amount of a species or assemblage that may be harvested or processed by a vessel or processing plant. Cumulative changes since 2014 have impacted the CGOA fisheries, resulting in difficulties harvesting and processing the trawl CV RP cooperative quota (CQ), especially later in the season as processors approach the limit of their current processing caps or close for seasonal maintenance. Seasonal fishing activity is the driving force for the planning of vessels and processing facility staff needs. Changes since 2021 to the CGOA flatfish market, and the loss of several shoreside processing facilities in Kodiak, have created the need for additional flexibility to allow the fishery to adapt to unforeseen challenges within

the fishery. These challenges could include rockfish processor shutdowns or impacts to the markets.

Seven unique Kodiak processors, each associated with a unique rockfish vessel cooperative, participated in the RP from 2012 through 2014. These rockfish cooperatives are voluntarily formed by permit harvesters and receive an exclusive harvest privilege to the groundfish species in the CGOA. One RP rockfish processor was acquired in 2014 by another RP processing company, reducing the total number of RP processors to six but leaving the number of RP cooperatives unchanged. Later, in 2018, an RP rockfish processor ceased processing and the associated RP cooperative disbanded. In 2020, a merger between RP processors, and a third RP processor deciding not to take any RP deliveries, reduced the total number to four RP processors. Processors are currently limited to processing 30 percent of the CQ. In late 2023, one of the four remaining RP processors announced the intent to sell the rockfish processing plant located in Kodiak, which may leave 10 percent of the TAC in the water.

Amendment 113 would provide additional flexibility for vessels to participate in the RP during April, and

could keep RP processors fully operational, thus mitigating impacts from changes in market conditions. Since 2021, the CGOA flatfish market prices have declined, partially due to increased tariffs, negatively impacting Kodiak processors financially due to labor planning and lack of sustained deliveries to keep processing crews active. The change in season start date would likely help maintain processing capacity for other non-trawl fisheries through workforce stability, which was observed during the 2021 rockfish season under the emergency rule (86 FR 14851, March 19, 2021), which moved the season start date to April 1, 2021. Changes to RP processor use caps would remove processing cap constraints while still maintaining the Council's original intent of preventing consolidation and meeting the overall goal of prosecuting this fishery in a sustainable and efficient manner. These changes to the regulations would provide additional opportunity for the TACs for the primary rockfish and other allocated species to be fully harvested, as indicated by the Council's purpose and need statement.

NMFS is soliciting public comments on proposed Amendment 113 through the end of the comment period (see

DATES). NMFS intends to publish in the **Federal Register** and seek public comment on a proposed rule that would implement Amendment 113 following NMFS's evaluation of the proposed rule under the Magnuson-Stevens Act.

Respondents do not need to submit the same comments on Amendment 113 and the proposed rule. All relevant written comments received by the end of the applicable comment period, whether specifically directed to the FMP amendment or the proposed rule, will be considered by NMFS in the approval/disapproval decision for Amendment 113 and addressed in the response to comments in the final rule. Comments received after that date may not be considered in the approval/disapproval decision on Amendment 113. To be certain of consideration, comments must be received, not just postmarked or otherwise transmitted, by the last day of the comment period (see **DATES**).

Authority: 16 U.S.C. 1801 *et seq.*

Dated: March 29, 2024.

Everett Wayne Baxter,
Acting Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 2024-07115 Filed 4-3-24; 8:45 am]

BILLING CODE 3510-22-P

Notices

Federal Register

Vol. 89, No. 66

Thursday, April 4, 2024

This section of the FEDERAL REGISTER contains documents other than rules or proposed rules that are applicable to the public. Notices of hearings and investigations, committee meetings, agency decisions and rulings, delegations of authority, filing of petitions and applications and agency statements of organization and functions are examples of documents appearing in this section.

DEPARTMENT OF AGRICULTURE

Animal and Plant Health Inspection Service

[Docket No. APHIS–2023–0040]

Notice of Availability of Pest Risk Analyses for the Importation of Rosemary and Tarragon From Ethiopia Into the Continental United States

AGENCY: Animal and Plant Health Inspection Service, USDA.

ACTION: Notice of availability.

SUMMARY: We are advising the public that we have prepared pest risk analyses that evaluate the risks associated with the importation of leaves and stems of rosemary and leaves and stems of tarragon from Ethiopia into the continental United States. Based on the analyses, we have determined that the application of one or more designated phytosanitary measures will be sufficient to mitigate the risks of introducing or disseminating plant pests or noxious weeds via the importation of rosemary and tarragon from Ethiopia. We are making the pest risk analyses available to the public for review and comment.

DATES: We will consider all comments that we receive on or before June 3, 2024.

ADDRESSES: You may submit comments by either of the following methods:

- *Federal eRulemaking Portal:* Go to www.regulations.gov. Enter APHIS–2023–0040 in the Search field. Select the Documents tab, then select the Comment button in the list of documents.
- *Postal Mail/Commercial Delivery:* Send your comment to Docket No. APHIS–2023–0040, Regulatory Analysis and Development, PPD, APHIS, Station 3A–03.8, 4700 River Road, Unit 118, Riverdale, MD 20737–1238.

Supporting documents and any comments we receive on this docket

may be viewed at www.regulations.gov or in our reading room, which is located in Room 1620 of the USDA South Building, 14th Street and Independence Avenue SW, Washington, DC. Normal reading room hours are 8 a.m. to 4:30 p.m., Monday through Friday, except holidays. To be sure someone is there to help you, please call (202) 799–7039 before coming.

FOR FURTHER INFORMATION CONTACT: Ms. Gina Stiltner, Senior Regulatory Policy Specialist, Regulatory Coordination and Compliance, PPQ, APHIS, 4700 River Road, Unit 133, Riverdale, MD 20737–1231; (518) 760–2468; Gina.L.Stiltner@USDA.gov.

SUPPLEMENTARY INFORMATION:

Background

Under the regulations in “Subpart L—Fruits and Vegetables” (7 CFR 319.56–1 through 319.56–12, referred to below as the regulations), the Animal and Plant Health Inspection Service (APHIS) prohibits or restricts the importation of fruits and vegetables into the United States from certain parts of the world to prevent plant pests from being introduced into or disseminated within the United States.

Section 319.56–4 contains a performance-based process for approving the importation of fruits and vegetables that, based on the findings of a pest risk analysis, can be safely imported subject to one or more of the five designated phytosanitary measures listed in paragraph (b) of that section.

APHIS received a request from the national plant protection organization of Ethiopia to allow the importation of leaves and stems of rosemary (*Rosmarinus officinalis*) and leaves and stems of tarragon (*Artemisia dracunculus*) from Ethiopia into the continental United States. As part of our evaluation of Ethiopia’s request, we have prepared pest risk assessments to identify the pests of quarantine significance that could follow the pathway of the importation of rosemary and tarragon into the continental United States from Ethiopia. Based on the pest risk assessments, risk management documents (RMDs) were prepared to identify phytosanitary measures that could be applied to the rosemary and tarragon to mitigate the pest risk.

Therefore, in accordance with § 319.56–4(c), we are announcing the availability of our pest risk assessments

and RMDs for public review and comment. Those documents, as well as a description of the economic considerations associated with the importation of rosemary and tarragon from Ethiopia, may be viewed on the Regulations.gov website or in our reading room (see **ADDRESSES** above for a link to Regulations.gov and information on the location and hours of the reading room). You may request paper copies of the pest risk assessments and RMDs by calling or writing to the person listed under **FOR FURTHER INFORMATION CONTACT**. Please refer to the subject of the analysis you wish to review when requesting copies.

After reviewing any comments we receive, we will announce our decision regarding the import status of rosemary and tarragon from Ethiopia in a subsequent notice. If the overall conclusions of our analysis and the Administrator’s determination of risk remain unchanged following our consideration of the comments, then we will authorize the importation of rosemary and tarragon from Ethiopia into the continental United States subject to the requirements specified in the RMDs. Depending on the comments received, we may authorize the importation of all, some, or none of the commodities from Ethiopia specified in this notice.

Authority: 7 U.S.C. 1633, 7701–7772, and 7781–7786; 21 U.S.C. 136 and 136a; 7 CFR 2.22, 2.80, and 371.3.

Done in Washington, DC, this 26th day of March 2024.

Michael Watson,

Administrator, Animal and Plant Health Inspection Service.

[FR Doc. 2024–07104 Filed 4–3–24; 8:45 am]

BILLING CODE 3410–34–P

DEPARTMENT OF AGRICULTURE

Food Safety and Inspection Service

[Docket No. FSIS–2024–0004]

Notice of Request To Renew an Approved Information Collection: Voluntary Recalls of Meat, Poultry, and Egg Products

AGENCY: Food Safety and Inspection Service (FSIS), U.S. Department of Agriculture (USDA).

ACTION: Notice and request for comments.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995 and Office of Management and Budget (OMB) regulations, FSIS is announcing its intention to renew an approved information collection regarding voluntary recalls from commerce of meat, poultry, and egg products. There are no changes to the existing information collection. The approval for this information collection will expire on September 30, 2024.

DATES: Submit comments on or before June 3, 2024.

ADDRESSES: FSIS invites interested persons to submit comments on this **Federal Register** notice. Comments may be submitted by one of the following methods:

- *Federal eRulemaking Portal:* This website provides commenters the ability to type short comments directly into the comment field on the web page or to attach a file for lengthier comments. Go to <https://www.regulations.gov>. Follow the on-line instructions at that site for submitting comments.

- *Mail:* Send to Docket Clerk, U.S. Department of Agriculture, Food Safety and Inspection Service, 1400 Independence Avenue SW, Mailstop 3758, Washington, DC 20250-3700.

- *Hand- or Courier-Delivered Submittals:* Deliver to 1400 Independence Avenue SW, Jamie L. Whitten Building, Room 350-E, Washington, DC 20250-3700.

Instructions: All items submitted by mail or electronic mail must include the Agency name and docket number FSIS-2024-0004. Comments received in response to this docket will be made available for public inspection and posted without change, including any personal information, to <https://www.regulations.gov>.

Docket: For access to background documents or comments received, call 202-720-5046 to schedule a time to visit the FSIS Docket Room at 1400 Independence Avenue SW, Washington, DC 20250-3700.

FOR FURTHER INFORMATION CONTACT: Gina Kouba, Office of Policy and Program Development, Food Safety and Inspection Service, USDA, 1400 Independence Avenue SW, Mailstop 3758, South Building, Washington, DC 20250-3700; 202-720-5046.

SUPPLEMENTARY INFORMATION:

Title: Voluntary Recalls of Meat, Poultry, and Egg Products.

OMB Number: 0583-0144.

Type of Request: Renewal of an approved information collection.

Abstract: FSIS has been delegated the authority to exercise the functions of the Secretary (7 CFR 2.18, 2.53), as specified

in the Federal Meat Inspection Act (FMIA) (21 U.S.C. 601, *et seq.*), and the Poultry Products Inspection Act (PPIA) (21 U.S.C. 451, *et seq.*), and the Egg Products Inspection Act (EPIA) (21 U.S.C. 1031, *et seq.*). These statutes mandate that FSIS protect the public by verifying that meat, poultry, and egg products are safe, wholesome, unadulterated, and properly labeled.

FSIS is requesting renewal of an approved information collection regarding voluntary recalls from commerce of meat, poultry, and egg products. There are no changes to the existing information collection. The approval for this information collection will expire on September 30, 2024.

FSIS may request that a firm that has produced or imported meat, poultry, or egg products that are adulterated or misbranded and has distributed such products in commerce recall the products in question. When there is a recall, FSIS asks that the recalling firm (*e.g.*, a manufacturer, distributor, or importer of record) provide the Agency with basic information, including the identity of the recalled product, the reason for the recall, and information about the distributors and retail consignees to whom the product was shipped. Under the FMIA, firms are required to keep such records that fully and correctly disclose all transactions in their business (21 U.S.C. 642). Under the PPIA, firms are required to keep such records as are properly necessary for the effective enforcement of the PPIA (21 U.S.C. 460(b)).

Industry representatives use the FSIS Form 5020-3 *FSIS Preliminary Inquiry Worksheet* to provide contact information and specific details regarding adulterated or misbranded product in commerce, including product identifiers, product amounts and supplemental information. Recalling firms and distributors then use the FSIS Form 5020-4 *FSIS Recall Distribution Information Template* to provide the location and contact information of consignees who received recalled product.

When a firm voluntarily recalls a product, FSIS conducts recall effectiveness checks. In conducting recall effectiveness checks, if the recall is to the retail or consumer level, the Agency contacts the distributors and retail consignees to ensure that they were notified of the recall, to verify the amount of product they received, and to confirm that they are removing the product from commerce and returning it to the recalling firm or otherwise disposing of the product.

FSIS has made the following estimates based upon an information collection assessment.

Estimate of Burden: FSIS estimates that it will take respondents an average of approximately 1.08 hours to collect and make this information available to FSIS.

Respondents: Official establishments, importers of record, and retail consignees.

Estimated Number of Respondents: 6,090.

Estimated Number of Responses per Respondent: 1.

Estimated Total Annual Burden on Respondents: 6,600 hours.

All responses to this notice will be summarized and included in the request for OMB approval. All comments will also become a matter of public record. Copies of this information collection assessment can be obtained from Gina Kouba, Office of Policy and Program Development, Food Safety and Inspection Service, USDA, 1400 Independence Avenue SW, Mailstop 3758, South Building, Washington, DC 20250-3700; 202-720-5046.

Comments are invited on: (a) whether the proposed collection of information is necessary for the proper performance of FSIS' functions, including whether the information will have practical utility; (b) the accuracy of FSIS' estimate of the burden of the proposed collection of information, including the validity of the method and assumptions used; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques, or other forms of information technology. Comments may be sent to both FSIS, at the addresses provided above, and the Desk Officer for Agriculture, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB), Washington, DC 20253.

Additional Public Notification

Public awareness of all segments of rulemaking and policy development is important. Consequently, FSIS will announce this **Federal Register** publication on-line through the FSIS web page located at: <https://www.fsis.usda.gov/federal-register>.

FSIS will also announce and provide a link to this **Federal Register** publication through the FSIS *Constituent Update*, which is used to provide information regarding FSIS policies, procedures, regulations, **Federal Register** notices, FSIS public

meetings, and other types of information that could affect or would be of interest to our constituents and stakeholders. The *Constituent Update* is available on the FSIS web page. Through the web page, FSIS can provide information to a much broader, more diverse audience. In addition, FSIS offers an email subscription service which provides automatic and customized access to selected food safety news and information. This service is available at: <https://www.fsis.usda.gov/subscribe>. Options range from recalls to export information, regulations, directives, and notices. Customers can add or delete subscriptions themselves and have the option to password protect their accounts.

USDA Non-Discrimination Statement

In accordance with Federal civil rights law and USDA civil rights regulations and policies, USDA, its Mission Areas, agencies, staff offices, employees, and institutions participating in or administering USDA programs are prohibited from discriminating based on race, color, national origin, religion, sex, gender identity (including gender expression), sexual orientation, disability, age, marital status, family/parental status, income derived from a public assistance program, political beliefs, or reprisal or retaliation for prior civil rights activity, in any program or activity conducted or funded by USDA (not all bases apply to all programs). Remedies and complaint filing deadlines vary by program or incident.

Program information may be made available in languages other than English. Persons with disabilities who require alternative means of communication to obtain program information (e.g., Braille, large print, audiotape, American Sign Language) should contact the responsible Mission Area, agency, or staff office; the USDA TARGET Center at (202) 720-2600 (voice and TTY); or the Federal Relay Service at (800) 877-8339.

To file a program discrimination complaint, a complainant should complete a Form AD-3027, *USDA Program Discrimination Complaint Form*, which can be obtained online at <https://www.usda.gov/forms/electronic-forms>, from any USDA office, by calling (866) 632-9992, or by writing a letter addressed to USDA. The letter must contain the complainant's name, address, telephone number, and a written description of the alleged discriminatory action in sufficient detail to inform the Assistant Secretary for Civil Rights (ASCR) about the nature and date of an alleged civil rights

violation. The completed AD-3027 form or letter must be submitted to USDA by:

(1) *Mail*: U.S. Department of Agriculture, Office of the Assistant Secretary for Civil Rights, 1400 Independence Avenue SW, Washington, DC 20250-9410;

(2) *Fax*: (833) 256-1665 or (202) 690-7442; or

(3) *Email*: program.intake@usda.gov.
USDA is an equal opportunity provider, employer, and lender.

Paul Kiecker,
Administrator.

[FR Doc. 2024-07127 Filed 4-3-24; 8:45 am]

BILLING CODE 3410-DM-P

DEPARTMENT OF AGRICULTURE

Food and Nutrition Service

Agency Information Collection Activities, Proposed Collection: Request for Comments on Evaluating the Interview Requirement for Supplemental Nutrition Assistance Program (SNAP) Certification Study

AGENCY: Food and Nutrition Service (FNS), USDA.

ACTION: Notice.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995, this notice invites the general public and other public agencies to comment on this proposed information collection. This is a new information collection for the contract of the study titled "Evaluating the Interview Requirement for SNAP Certification." The purpose of this collection is to help FNS describe the effects of waiving the interview requirement, including SNAP agency processes and staff experiences with implementing the no-interview demonstration, analyzing the differences in outcomes for SNAP applicants and recipients, and identifying key lessons to inform future policy or implementation.

DATES: Written comments must be received on or before June 3, 2024.

ADDRESSES: Comments may be mailed to Amanda Wyant, Food and Nutrition Service, U.S. Department of Agriculture, 1320 Braddock Place, 5th Floor, Alexandria, VA 22314. Comments may also be submitted via email to Amanda.Wyant@usda.gov. Comments will also be accepted through the Federal eRulemaking Portal. Go to <http://www.regulations.gov>, and follow the online instructions for submitting comments electronically.

All responses to this notice will be summarized and included in the request for Office of Management and Budget

approval. All comments will be a matter of public record.

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of this information collection should be directed to Amanda Wyant at 703-305-7537.

SUPPLEMENTARY INFORMATION: Comments are invited on (a) whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions that were used; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on those who are to respond, including use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Title: Evaluating the Interview Requirement for SNAP Certification Study.

Form Number: N/A.

OMB Number: 0584-NEW.

Expiration Date: Not yet determined.

Type of Request: New collection.

Abstract: The Supplemental Nutrition Assistance Program (SNAP) is the foundation of the nation's nutrition assistance safety net and is a core source of support to millions of Americans, particularly during economic downturns. To help States handle increased need and participation amid the health risks of the pandemic, the Food and Nutrition Service (FNS) offered States a range of flexibilities which provided support to States administering the program and clients in the application process, including the option to waive the certification and recertification interview requirement. This allowed States to continue administering SNAP during the public health emergency with minimal client contact. FNS required States that waived the interview requirement to document their experiences processing cases without the interview. However, more rigorous evidence is needed to confidently understand the effects of waiving the interview requirement.

The Evaluating the Interview Requirement for SNAP Certification study will collect information in five States to assess how eliminating interviews affects outcomes, including administrative efficiency, costs, benefit accuracy, and client access. The project

will include a randomized control trial (RCT) to analyze the impacts of outcomes between those clients assigned to receive an interview (the regular interview process group) and those assigned to not receive an interview (the no-interview group). The project will also include collection of administrative and quality control data, as well as qualitative information. The qualitative data collection will include virtual site visits and observations, a workflow analysis, and a time-use study. During the site visits, the team will conduct interviews with staff involved with all stages of certification and recertification processes. Site visitors will observe verification calls between eligibility workers and no-interview SNAP applicants to collect information about whether staff carry out policies and procedures as intended. The workflow analysis will involve small group interviews with State and local staff and will support the assessment of the changes required when implementing the no-interview demonstration and the possible challenges. Finally, the study will include a staff time-use survey to determine whether application processing requires more or less time for workers when there is an interview compared to when there is not.

Affected public. Members of the public affected by the data collection include State and local government workers from SNAP agencies in five States, as well as staff at not-for-profit organizations, and individuals who apply for or participate in SNAP. Respondent groups identified include (1) State SNAP directors, (2) State SNAP policy directors, (3) State SNAP field operations managers, (4) State data systems staff, (5) State quality control (QC) staff, (6) local SNAP directors, (7) local SNAP office supervisors, (8) eligibility workers, (9) customer service staff, (10) community based organizations (CBOs) and advocates, and (11) SNAP applicants and participants.

Estimated number of respondents. The total estimated number of unique respondents—which includes everyone contacted for data collection regardless of whether they participate—is 494.

This includes up to 65 individuals/households, 409 State and local government staff, and 20 community based organization staff or advocates. The study team will contact 65 individuals/households, out of which 50 SNAP applicants or participants will participate in an observation and 15 SNAP applicants or participants will be considered nonrespondents. The study team will contact 63 State SNAP agency staff, which includes SNAP directors, SNAP policy directors, State SNAP field operations managers, State data systems staff, and State QC staff. The study team will contact 67 local agency directors/supervisors, out of which 20 will be considered nonrespondents. The study team will contact 279 local agency direct service staff, out of which 80 will be considered nonrespondents. Fifteen of the State directors will provide administrative data. The study team will contact 20 community based organizations or advocates for virtual interviews.

Respondents will participate in multiple activities as follows:

- 5 State SNAP directors (one from each State will participate in the interviews and workflow analysis)
- 5 State SNAP policy directors (one from each State will participate in the interviews, document review and workflow analysis)
- 20 State field operations managers (four from each State will participate in the interviews and workflow analysis)
- 15 State data systems staff (three from each State will participate in the interviews, workflow analysis, and administrative data collection)
- 15 Local SNAP directors (three from each State will participate in the interviews and work flow analysis)
- 30 Local SNAP office supervisors (6 from each State will participate in the time-use survey, workflow analysis, and/or the interviews)
- 135 Eligibility workers (27 from each State will participate in the time-use survey, observations, workflow analysis, and/or interviews. Eligibility workers could participate in one or multiple activities in the study. Amongst the 135 eligibility workers, 90 will have participated in the time-

use survey, 50 will have participated in the observations, 45 will have participated in the interviews, and 30 will have participated in the workflow analysis)

- 60 customer service staff (12 from each State will participate in the time-use survey, workflow analysis, and/or the interviews. Customer service staff could participate in the time-use survey and the interviews or the interviews and observations or only one of these activities. Amongst the 60 customer service staff, 30 will have participated in the time-use survey, 30 will have participated in the workflow analysis, and 30 will have participated in the interviews)

The 15 State QC staff will participate in the interviews. Before the start of data collection in one non-study State, we will pretest the semi-structured interview guide with one State SNAP director, one State SNAP policy director, one State data system staff, one Local SNAP director, one eligibility worker, and one customer service staff member. We also will pretest the time-use survey with one eligibility worker, one customer service staff, and one Local SNAP office supervisor.

Estimated number of responses per respondent. Across all 494 unique respondents (379 respondents and 115 non-respondents) and 3,159 annual responses, the average number of responses is 6.39.

Estimated total annual responses. 3,159.

Estimated time per response. The time per all respondent/non-respondent group was used to determine the annual frequency estimates. The estimated time per response varies from 0.0835 hours for activities related to reading email reminders for the time-use survey to 24 hours for State data systems staff to provide administrative data. The response time will vary depending on the respondent group, with an average estimated time of 105 minutes (1.75 hours).

Estimated total annual burden on respondents. The total estimated annual burden on respondents is 108,300 minutes (1,805 hours).

BILLING CODE 3410-30-P

Affected public	Type of respondents	Instruments	RESPONDENTS						NON-RESPONDENTS						Grand total annual burden estimate (hours)	Hourly Wage rate*	Total cost with fringe benefits (33%)	Total annualized cost of respondent burden
			Sample size	Number of respondents	Frequency of response	Total annual responses	Hours per response	Annual burden (hours)	Number of non-respondents	Frequency of response	Total annual responses	Hours per response	Annual burden (hours)					
State/Local Government	State Data Systems Staff	Administrative data	15	15	1	15	24.00	360.00	0	0	0	0.00	0.00	360.00	\$51.99	-	\$18,716.40	
State/Local Government	State SNAP Policy Director	Document review	5	5	1	5	0.50	2.50	0	0	0	0.00	0.00	2.50	83.18	-	\$207.95	
State/Local Government	Eligibility Worker	Observations	50	50	1	50	0.58	29.17	0	0	0	0.00	0.00	29.17	26.08	-	\$760.67	
State/Local Government	State SNAP Director	Semi-structured Interview	5	5	1	5	1.25	6.25	0	0	0	0.00	0.00	6.25	83.18	-	\$519.88	
State/Local Government	State SNAP Policy Director	Semi-structured Interview	5	5	1	5	1.25	6.25	0	0	0	0.00	0.00	6.25	83.18	-	\$519.88	
State/Local Government	State Field Operations Manager	Semi-structured Interview	20	20	1	20	1.25	25.00	0	0	0	0.00	0.00	25.00	52.14	-	\$1,303.50	
State/Local Government	State Data Systems Staff	Semi-structured Interview	15	15	1	15	1.25	18.75	0	0	0	0.00	0.00	18.75	51.99	-	\$974.81	
State/Local Government	State QC Staff	Semi-structured Interview	15	15	1	15	1.25	18.75	0	0	0	0.00	0.00	18.75	51.99	-	\$974.81	
State/Local Government	Local SNAP Director	Semi-structured Interview	15	15	1	15	1.25	18.75	0	0	0	0.00	0.00	18.75	83.18	-	\$1,559.63	
State/Local Government	Local SNAP Office Supervisor	Semi-structured Interview	30	30	1	30	1.25	37.50	0	0	0	0.00	0.00	37.50	83.18	-	\$3,119.25	
State/Local Government	Eligibility Worker	Semi-structured Interview	45	45	1	45	1.25	56.25	0	0	0	0.00	0.00	56.25	26.08	-	\$1,467.00	
State/Local Government	Customer Service Staff	Semi-structured Interview	30	30	1	30	1.25	37.50	0	0	0	0.00	0.00	37.50	19.80	-	\$742.50	
State/Local Government	State SNAP Director	Semi-structured Interview	1	1	1	1	1.75	1.75	0	0	0	0.00	0.00	1.75	83.18	-	\$145.57	
State/Local Government	State SNAP Policy Director	Semi-structured Interview	1	1	1	1	1.75	1.75	0	0	0	0.00	0.00	1.75	83.18	-	\$145.57	
State/Local Government	State Data Systems Staff	Semi-structured Interview	1	1	1	1	1.75	1.75	0	0	0	0.00	0.00	1.75	51.99	-	\$90.98	
State/Local Government	Local SNAP Director	Semi-structured Interview	1	1	1	1	1.75	1.75	0	0	0	0.00	0.00	1.75	83.18	-	\$145.57	

State/Local Government	Eligibility Worker	Semi-structured Interview pretest	1	1	1	1	1.75	1.75	0	0	0	0.00	0.00	1.75	26.08	-	\$45.64
State/Local Government	Customer Service Staff	Semi-structured Interview pretest	1	1	1	1	1.75	1.75	0	0	0	0.00	0.00	1.75	19.80	-	\$34.65
State/Local Government	Local SNAP Office Supervisor	Time-use survey	30	30	5	150	0.75	112.50	0	0	0	0.00	0.00	112.50	52.14	-	\$5,865.75
State/Local Government	Eligibility Worker	Time-use survey	90	90	5	450	0.75	337.50	0	0	0	0.00	0.00	337.50	26.08	-	\$8,802.00
State/Local Government	Customer Service Staff	Time-use survey	30	30	5	150	0.75	112.50	0	0	0	0.00	0.00	112.50	19.80	-	\$2,227.50
State/Local Government	Local SNAP Office Supervisor	Time-use survey daily afternoon reminder email	30	30	5	150	0.08	12.50	0	0	0	0.00	0.00	12.50	52.14	-	\$651.75
State/Local Government	Eligibility Worker	Time-use survey daily afternoon reminder email	90	90	5	450	0.08	37.50	0	0	0	0.00	0.00	37.50	26.08	-	\$978.00
State/Local Government	Customer Service Staff	Time-use survey daily afternoon reminder email	30	30	5	150	0.08	12.50	0	0	0	0.00	0.00	12.50	19.80	-	\$247.50
State/Local Government	Local SNAP Office Supervisor	Time-use survey daily morning email	30	30	5	150	0.08	12.50	0	0	0	0.00	0.00	12.50	52.14	-	\$651.75
State/Local Government	Eligibility Worker	Time-use survey daily morning email	90	90	5	450	0.08	37.50	0	0	0	0.00	0.00	37.50	26.08	-	\$978.00
State/Local Government	Customer Service Staff	Time-use survey daily morning email	30	30	5	150	0.08	12.50	0	0	0	0.00	0.00	12.50	19.80	-	\$247.50
State/Local Government	Local SNAP Office Supervisor	Time-use survey instructional email	50	30	1	30	0.17	5.00	20	1	20	0.17	3.33	8.33	52.14	-	\$434.50
State/Local Government	Eligibility Worker	Time-use survey instructional email	150	90	1	90	0.17	15.00	60	1	60	0.17	10.00	25.00	26.08	-	\$652.00
State/Local Government	Customer Service Staff	Time-use survey instructional email	50	30	1	30	0.17	5.00	20	1	20	0.17	3.33	8.33	19.80	-	\$165.00
State/Local Government	Local SNAP Office Supervisor	Time-use survey pretest	1	1	1	1	0.75	0.75	0	0	0	0.00	0.00	0.75	83.18	-	\$62.39
State/Local Government	Eligibility Worker	Time-use survey pretest	1	1	5	5	0.75	3.75	0	0	0	0.00	0.00	3.75	26.08	-	\$97.80
State/Local Government	Customer Service Staff	Time-use survey pretest	1	1	5	5	0.75	3.75	0	0	0	0.00	0.00	3.75	19.80	-	\$74.25

State/Local Government	Local SNAP Office Supervisor	Time-use survey pretest afternoon reminder email	1	1	1	1	0.08	0.08	0	0	0	0.00	0.00	0.08	83.18	-	\$6.93
State/Local Government	Eligibility Worker	Time-use survey pretest afternoon reminder email	1	1	1	1	0.08	0.08	0	0	0	0.00	0.00	0.08	26.08	-	\$2.17
State/Local Government	Customer Service Staff	Time-use survey pretest afternoon reminder email	1	1	1	1	0.08	0.08	0	0	0	0.00	0.00	0.08	19.80	-	\$1.65
State/Local Government	Local SNAP Office Supervisor	Time-use survey pretest instructional email	1	1	1	1	0.17	0.17	0	0	0	0.00	0.00	0.17	83.18	-	\$13.86
State/Local Government	Eligibility Worker	Time-use survey pretest instructional email	1	1	1	1	0.17	0.17	0	0	0	0.00	0.00	0.17	26.08	-	\$4.35
State/Local Government	Customer Service Staff	Time-use survey pretest instructional email	1	1	1	1	0.17	0.17	0	0	0	0.00	0.00	0.17	19.80	-	\$3.30
State/Local Government	Local SNAP Office Supervisor	Time-use survey pretest morning email	1	1	1	1	0.08	0.08	0	0	0	0.00	0.00	0.08	83.18	-	\$6.93
State/Local Government	Eligibility Worker	Time-use survey pretest morning email	1	1	1	1	0.08	0.08	0	0	0	0.00	0.00	0.08	26.08	-	\$2.17
State/Local Government	Customer Service Staff	Time-use survey pretest morning email	1	1	1	1	0.08	0.08	0	0	0	0.00	0.00	0.08	19.80	-	\$1.65
State/Local Government	Local SNAP Office Supervisor	Time-use survey pretest staff questionnaire	1	1	1	1	0.17	0.17	0	0	0	0.00	0.00	0.17	83.18	-	\$13.86
State/Local Government	Eligibility Worker	Time-use survey pretest staff questionnaire	1	1	1	1	0.17	0.17	0	0	0	0.00	0.00	0.17	26.08	-	\$4.35
State/Local Government	Customer Service Staff	Time-use survey pretest staff questionnaire	1	1	1	1	0.17	0.17	0	0	0	0.00	0.00	0.17	19.80	-	\$3.30
State/Local Government	Local SNAP Office Supervisor	Time-use survey staff questionnaire	30	30	1	30	0.17	5.00	0	0	0	0.00	0.00	5.00	52.14	-	\$260.70
State/Local Government	Eligibility Worker	Time-use survey staff questionnaire	90	90	1	90	0.17	15.00	0	0	0	0.00	0.00	15.00	26.08	-	\$391.20
State/Local Government	Customer Service Staff	Time-use survey staff questionnaire	30	30	1	30	0.17	5.00	0	0	0	0.00	0.00	5.00	19.80	-	\$99.00

State/Local Government	State SNAP Director	Workflow analysis group interview	5	5	1	5	2.50	12.50	0	0	0	0.00	0.00	12.50	83.18	-	\$1,039.75
State/Local Government	State SNAP Policy Director	Workflow analysis group interview	5	5	1	5	2.50	12.50	0	0	0	0.00	0.00	12.50	83.18	-	\$1,039.75
State/Local Government	State SNAP Field Operations Manager	Workflow analysis group interview	15	15	1	15	2.50	37.50	0	0	0	0.00	0.00	37.50	52.14	-	\$1,955.25
State/Local Government	State Data Systems Staff	Workflow analysis group interview	15	15	1	15	2.50	37.50	0	0	0	0.00	0.00	37.50	51.99	-	\$1,949.63
State/Local Government	Local SNAP Director	Workflow analysis group interview	15	15	1	15	2.50	37.50	0	0	0	0.00	0.00	37.50	83.18	-	\$3,119.25
State/Local Government	Local SNAP Office Supervisor	Workflow analysis group interview	30	30	1	30	2.50	75.00	0	0	0	0.00	0.00	75.00	83.18	-	\$6,238.50
State/Local Government	Eligibility Worker	Workflow analysis group interview	30	30	1	30	2.50	75.00	0	0	0	0.00	0.00	75.00	26.08	-	\$1,956.00
State/Local Government	Customer Service Staff	Workflow analysis group interview	30	30	1	30	2.50	75.00	0	0	0	0.00	0.00	75.00	19.80	-	\$1,485.00
Not-for-Profit Organizations	Community based organizations (CBOs) and advocates	Semi-structured Interview	20	20	1	20	1.25	25.00	0	0	0	0.00	0.00	25.00	46.83	-	\$1,170.75
Individuals/Household	SNAP applicants and participants	Observations	65	50	1	50	0.50	25.00	15	1	15	0.08	1.25	26.25	7.25	-	\$190.31
Subtotal of unique State agency SNAP Staff			63	63	13	118	44	530.25	0	0	0	0.00	0.00	530.25	n/a	-	\$37,340
Subtotal of unique Local agency SNAP staff			346	246	87	2856	31	1206.67	100	3	100	0.50	16.67	1223.33	n/a	-	\$35,868
Subtotal of unique SNAP applicants and participants			20	20	1	20	1.25	25.00	0	0	0	0.00	0.00	25.00	n/a	-	\$1,171
Grand total			65	50	1	50	0.50	25.00	15	1	15	0.08	1.25	26.25	n/a	-	\$ 190
Grand total			494	379	102	3,044	76.08	1,787	115	4	115	0.58	17.92	1,804.83	n/a	\$99,178	\$74,570

Tameka Owens,

Assistant Administrator, Food and Nutrition Service.

[FR Doc. 2024-07164 Filed 4-3-24; 8:45 am]

BILLING CODE 3410-30-C

DEPARTMENT OF AGRICULTURE

Food and Nutrition Service

Agency Information Collection

Activities: Assessment of Administrative Costs of Electronic Healthy Incentives Projects (eHIP)

AGENCY: Food and Nutrition Service (FNS), USDA.

ACTION: Notice.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995, this notice invites the general public and other public agencies to comment on this proposed information collection. This is a new collection for the study "Assessment of Administrative Costs of Electronic Healthy Incentives Projects (eHIP)." This study will calculate costs incurred by eHIP, which will provide incentives through EBT integration to increase purchase of healthy foods (e.g., fruits and vegetables) by Supplemental Nutrition Assistance Program (SNAP) participants.

DATES: Written comments must be received on or before June 3, 2024.

ADDRESSES: Comments may be sent to: Kathleen Patton, Food and Nutrition Service, U.S. Department of Agriculture, 1320 Braddock Place, 5th Floor, Alexandria, VA 22314. Comments may also be submitted via email to Kathleen.Patton@usda.gov. Comments will also be accepted through the Federal eRulemaking Portal. Go to <http://www.regulations.gov> and follow the online instructions for submitting comments electronically.

All responses to this notice will be summarized and included in the request for Office of Management and Budget approval. All comments will be a matter of public record.

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of this information collection should be directed Kathleen Patton at Kathleen.Patton@usda.gov or 703-305-2813.

SUPPLEMENTARY INFORMATION: Comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden of the

proposed collection of information, including the validity of the methodology and assumptions that were used; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on those who are to respond, including use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Title: Assessment of Administrative Costs of Electronic Healthy Incentives Projects (eHIP).

Form Number: Not Applicable.

OMB Number: 0584-NEW.

Expiration Date: Not Yet Determined.

Type of Request: New Collection.

Abstract: The Supplemental Nutrition Assistance Program (SNAP), administered by the United States Department of Agriculture (USDA), Food and Nutrition Service (FNS), distributes benefits to eligible low-income households through Electronic Benefits Transfer (EBT) card technology. In fiscal year 2023 FNS awarded grants to three States, Colorado, Louisiana, and Washington for implementing Electronic Healthy Incentives Projects (eHIP) to leverage EBT integration to deliver financial incentives at point of purchase to SNAP households when they purchase qualifying foods (e.g., fruits and vegetables). The aim of this study is to calculate the costs of eHIP in the three States to determine the startup and ongoing costs of administering incentives to SNAP households through EBT integration and to estimate the cost of administering eHIP at scale. The study will quantify startup and ongoing administrative costs to State grantees, retailers, and other eHIP stakeholders. It will also compare administrative costs to the amount of funding distributed as incentives.

Data will be collected from the three project States and multiple entities working with these States, including retailers, EBT processors, third-party processors (TPPs). These data will include both cost data, collected through cost data templates submitted to the States/entities, as well as interviews with State and other project representatives to contextualize the cost data. In addition, existing national data (such as SNAP caseloads and SNAP-authorized retailers) and State data from non-project States (such as State wage rates) will be examined in order to estimate the cost of nationwide expansion of eHIP. Lastly, data from select Gus Schumacher Nutrition Incentive Program (GusNIP) grantees—that do not use EBT integration for

delivering incentives to SNAP households for purchasing fruits and vegetables will be examined to estimate the costs and return on investment (ROI) of GusNIP and compare these to the eHIP costs and ROI, in order to provide information on how these two incentive delivery modalities differ in costs and economic impact.

Data collection is expected to occur beginning in March 2025 with an approximate end date of May 2026. Data collection activities will be designed to address the three main objectives for the study:

1. Quantify, to the extent possible, the cost of administering eHIP;
2. Estimate the cost of nationwide expansion of eHIP; and
3. Compare the cost of administering eHIP with other incentive programs for SNAP households that do not use EBT integration.

Design consists of building and populating a central cost model for estimating the costs of implementing and administering eHIP. This model will then be expanded, through the use of publicly available State and national data, to estimate the nationwide costs of implementation and administration. Finally, existing data on GusNIP programs will be used to compare costs between eHIP and GusNIP.

Affected Public: State respondents are eHIP project staff. For-profit and not-for-profit business respondents are eHIP-participating EBT vendor staff, TPP staff, and retailer staff.

Estimated Number of Respondents: The estimated number of respondents is 38. Within each State, the study expects responses from 4 State staff (4 staff × 3 States = 12 State staff). In addition, the study expects to have responses from 6 retailer staff for each eHIP State (6 staff × 3 States = 18 retailer staff), as well as 2 TPP staff for each eHIP State (2 staff × 3 States = 6 TPP staff). Finally, the study expects responses from 2 EBT processor staff, 1 each from the two EBT processor firms working with the three eHIP States.

Estimated Number of Responses per Respondent: Across all respondents, the average number of responses is 7.3 (277 responses across 38 respondent). The number of responses will vary by respondent group and the specific data collection activity.

For the State SNAP agency staff:

- One staffer within each State will be asked to respond once to the pre-test of the cost templates and three times to the cost data templates data collection.
- Two staffers in each State will be asked to respond twice to the phone interview data collection. Staff will receive an electronic letter (i.e., email)

for inviting them to participate and for scheduling the interview. They will also receive an email reminder for the interview, as well as a thank you email.

For the EBT processors, one staff from each of the two EBT processors will be asked to respond two times to phone interview data collection (including invitation to schedule, reminder, interview, and thank you note). For the retailer staff, 6 retailer staff from each State will be asked to respond two times to phone interview data collection (including invitation to schedule,

reminder, interview, and thank you note). For the TPP staff, two staff from each State will be asked to respond two times to phone interview data collection (including invitation to schedule, reminder, interview, and thank you note).

We expect a 100 percent response rate from all categories of respondents.

Estimated Total Annual Responses: The estimated number of total annual responses is 277 (38 respondents and no nonrespondents).

Estimated Time per Response: The estimated time of response varies from 0.083 hours to 7 hours depending on the instrument, as shown in the table below. The average estimated time per response is 0.644 hours.

Estimated Total Annual Burden on Respondents: The estimated total annual burden on respondents 178.315 hours. See the table below for estimated total annual burden for each type of respondent.

BILLING CODE 3410-30-P

Total Burden Estimates

Respondent Category	Type of respondents	Instruments	Sample Size	Responsive					Non-Responsive					All Respondents		
				Number of respondents	Frequency of response	Total Annual responses	Hours per response ^a	Annual burden (hours)	Number of non-respondents	Frequency of response	Total Annual responses	Hours per response	Annual burden (hours)	Grand Total Annual Burden Estimate (hours)	Hourly Wage Rate ^b	Total Annualized Cost of Respondent Burden ^c
		Pre-test with Cost Templates	3	3	1	3	1.5	4.5	0	0	0	0	0	4.5	\$ 40.85	\$ 183.83
State Government ^d	Project Staff	Electronic Letter with Data Request	3	3	3	9	0.167	1.503	0	0	0	0	0	1.503	\$ 40.85	\$ 61.40
		Cost Data Templates Data Collection	3	3	3	9	7	63	0	0	0	0	0	63	\$ 40.85	\$ 2,573.55
		Electronic Letter with Request to Schedule Phone Interview	6	6	2	12	0.167	2.004	0	0	0	0	0	2.004	\$ 40.85	\$ 81.86
		Electronic Letter with Reminder about Phone Interview	6	6	2	12	0.083	0.996	0	0	0	0	0	0.996	\$ 40.85	\$ 40.69
		In-Depth Phone Interview (includes consent)	6	6	2	12	1.5	18	0	0	0	0	0	18	\$ 40.85	\$ 735.30
		In-Depth Interview Follow Up and Thank You Note	6	6	2	12	0.083	0.996	0	0	0	0	0	0	0.996	\$ 40.85
State Sub-Total			12	12	6	69	1.3188261	90.999	0	0	0	0	0	90.999		\$ 3,717.31

Businesses	EBT Processors ^e	Electronic Letter with Request to Schedule Phone Interview	2	2	2	4	0.167	0.668	0	0	0	0	0	0.668	\$ 83.49	\$ 55.77
		Electronic Letter with Reminder about Phone Interview	2	2	2	4	0.083	0.332	0	0	0	0	0	0.332	\$ 83.49	\$ 27.72
		In-Depth Phone Interview (includes consent)	2	2	2	4	1	4	0	0	0	0	0	4	\$ 83.49	\$ 333.96
		In-Depth Interview Follow Up and Thank You Note	2	2	2	4	0.083	0.332	0	0	0	0	0	0.332	\$ 83.49	\$ 27.72
	Retailers ^f	Electronic Letter with Request to Schedule Phone Interview	18	18	2	36	0.167	6.012	0	0	0	0	0	6.012	\$ 59.07	\$ 355.13
		Electronic Letter with Reminder about Phone Interview	18	18	2	36	0.083	2.988	0	0	0	0	0	2.988	\$ 59.07	\$ 176.50
		In-Depth Phone Interview (includes consent)	18	18	2	36	1.5	54	0	0	0	0	0	54	\$ 59.07	\$ 3,189.78
		In-Depth Interview Follow Up and Thank You Note	18	18	2	36	0.083	2.988	0	0	0	0	0	2.988	\$ 59.07	\$ 176.50

Third Party Processors ^d	Electronic Letter with Request to Schedule Phone Interview	6	6	2	12	0.167	2.004	0	0	0	0	0	2.004	\$ 83.49	\$ 167.31
	Electronic Letter with Reminder about Phone Interview	6	6	2	12	0.083	0.996	0	0	0	0	0	0.996	\$ 83.49	\$ 83.16
	In-Depth Phone Interview (includes consent)	6	6	2	12	1	12	0	0	0	0	0	12	\$ 83.49	\$ 1,001.88
	In-Depth Interview Follow Up and Thank You Note	6	6	2	12	0.083	0.996	0	0	0	0	0	0.996	\$ 83.49	\$ 83.16
Business Sub-Total		26	26	6	208	0.4197885	87.316	0	0	0	0	0	65		\$ 5,678.59
TOTAL		38	38	12	277	0.6437365	178.315	0	0	0	0	0	178.315		\$ 9,395.90

Notes:

^aDecimal values have been calculated by multiplying the decimal unit value of one minute (.0167) by the total number of minutes (Conversion of Minutes to Decimals)

^bAll hourly wage rates are fully loaded.

^cCosts are rounded up to the next whole cent.

^dJob category "Management Occupations" code #11-9151 "Social and Community Service Managers" industry "State Government" for state level mean hourly wage of \$40.85.

^eJob category "Management Occupations" code #11-3021 "Computer and Information Systems Managers" mean hourly wage \$83.49.

^fJob category "Management Occupations" code #11-1021 "General and Operations Managers" mean hourly wage \$59.07.

Tameka Owens,

Assistant Administrator, Food and Nutrition Service.

[FR Doc. 2024-07163 Filed 4-3-24; 8:45 am]

BILLING CODE 3410-30-C

DEPARTMENT OF AGRICULTURE

Forest Service

Newspapers Used for Publication of Legal Notices by the Alaska Region

AGENCY: Forest Service, Agriculture (USDA).

ACTION: Notice.

SUMMARY: This notice lists the newspapers that will be used by the Ranger Districts, Forests, and Regional Office of the Alaska Region to publish legal notices required under Forest Service regulations. The intended effect of this action is to inform interested members of the public which newspapers the Forest Service will use to publish notices of proposed actions and notices of decision. This will provide the public with constructive notice of Forest Service proposals and decisions; provide information on the procedures to comment, object, or appeal; and establish the date that the Forest Service will use to determine if comments, appeals, or objections were timely.

DATES: This list of newspapers will remain in effect for one year from the date of publication when another notice will be published in the **Federal Register**.

ADDRESSES: Robin Dale, Alaska Region Group Leader for Administrative Reviews, Litigation, FOIA, Records, and Directives; Forest Service, Alaska Region; P.O. Box 21628; Juneau, Alaska 99802-1628.

FOR FURTHER INFORMATION CONTACT: Robin Dale; Alaska Region Group Leader for Administrative Reviews, Litigation, FOIA, Records, and Directives; (907) 586-9344 or robin.dale@usda.gov.

SUPPLEMENTARY INFORMATION: The administrative procedures at 36 CFR parts 218 and 219 require the Forest Service to publish notices in a newspaper of general circulation. The content of the notices is specified in 36 CFR parts 218 and 219. In general, the notices will identify: the decision or project by title or subject matter; the name and title of the official making the decision; how to obtain additional information; and where and how to file comments or appeals/objections. The date the notice is published will be used

to establish the official date for the beginning of the comment, appeal, or objection period. The newspapers to be used are as follows:

Alaska Regional Office

Decisions of the Alaska Regional Forester: *Juneau Empire*, published daily except Saturday and official holidays in Juneau, Alaska; and the *Anchorage Daily News*, published daily in Anchorage, Alaska.

Chugach National Forest

Decisions of the Chugach Forest Supervisor and the Glacier and Seward District Rangers: *Anchorage Daily News*, published daily in Anchorage, Alaska.

Decisions of the Cordova District Ranger: *Cordova Times*, published weekly in Cordova, Alaska.

Tongass National Forest

Decisions of the Tongass Forest Supervisor and the Craig, Ketchikan/Misty Fjords, and Thorne Bay District Rangers: *Ketchikan Daily News*, published daily except Sundays and official holidays in Ketchikan, Alaska.

Decisions of the Admiralty Island National Monument, the Juneau District Ranger, the Hoonah District Ranger, and the Yakutat District Ranger: *Juneau Empire*, published daily except Saturday and official holidays in Juneau, Alaska.

Decisions of the Petersburg District Ranger: *Petersburg Pilot*, published weekly in Petersburg, Alaska.

Decisions of the Sitka District Ranger: *Daily Sitka Sentinel*, published daily except Saturday, Sunday, and official holidays in Sitka, Alaska.

Decisions of the Wrangell District Ranger: *Wrangell Sentinel*, published weekly in Wrangell, Alaska.

Supplemental notices may be published in any newspaper, but the timeframes for filing objections will be calculated based upon the date that legal notices are published in the newspapers of record listed in this notice.

Dated: March 29, 2024.

Troy Heithecker,

Associate Deputy Chief, National Forest System.

[FR Doc. 2024-07119 Filed 4-3-24; 8:45 am]

BILLING CODE 3411-15-P

DEPARTMENT OF AGRICULTURE

Forest Service

Newspapers Used for Publication of Legal Notices by the Pacific Northwest Region, Oregon, Washington, and Parts of California

AGENCY: Forest Service, Agriculture (USDA).

ACTION: Notice of newspapers of record.

SUMMARY: This notice lists the newspapers that will be used by the ranger districts, national forests, and the regional office of the Pacific Northwest Region to publish legal notices required under the Code of Federal Regulations (CFR). The intended effect of this action is to inform interested members of the public which newspapers the Forest Service will use to publish notices of proposed actions and notices of decision. This will provide the public with constructive notice of Forest Service proposals and decisions; provide information on the procedures to comment, object or appeal; and establish the date that the Forest Service will use to determine if comments or appeals/objections were timely.

DATES: The list of newspapers will remain in effect for one year from the date of publication when another notice will be published in the **Federal Register**.

ADDRESSES: Christine Pyle, Program Specialist, Pacific Northwest Region, 1220 Southwest Third Avenue, Portland, OR 97204.

FOR FURTHER INFORMATION CONTACT: Christine Pyle, Program Specialist, Pacific Northwest Region, by telephone at 971-245-0269 or by email at Christine.pyle@usda.gov.

SUPPLEMENTARY INFORMATION: The administrative procedures at 36 CFR 214, 218, and 219 require the Forest Service to publish notices in a newspaper of general circulation. The content of the notices is specified in 36 CFR 214, 218, and 219. In general, the notices will identify: the decision or project by title or subject matter; the name and title of the official making the decision; how to obtain additional information; and where and how to file comments or appeals/objections. The date the notice is published will be used to establish the official date for the beginning of the comment or appeal/objection period.

The newspapers to be used are as follows:

Regional Forester, Pacific Northwest Region

Regional Forester decisions affecting National Forests in Oregon: *The Oregonian*.

Regional Forester decisions affecting National Forests in Washington: *The Seattle Times*.

Regional Forester decisions that affect all National Forests and Grasslands in the Pacific Northwest Region: *The Oregonian* and *The Seattle Times*.

Columbia River Gorge Scenic Area

Columbia River Gorge Area Manager/Forest Supervisor decisions: *Columbia Gorge News*.

Colville National Forest

Colville Forest Supervisor decisions: *Statesman-Examiner*.

Three Rivers District Ranger decisions: *Statesman-Examiner*.

Tonasket District Ranger decisions: *The Omak-Okanogan County Chronicle*.

Sullivan Lake District Ranger decisions: *The Newport Miner*.

Republic District Ranger decisions: *Ferry County View*.

Deschutes National Forest

Deschutes Forest Supervisor, District Ranger, and Redmond Air Center Manager decisions: *The Bulletin*.

Fremont-Winema National Forest

Fremont-Winema Forest Supervisor and District Ranger decisions: *Herald and News*.

Gifford Pinchot National Forest

Gifford Pinchot Forest Supervisor and Mount Saint Helens National Volcanic Monument decisions: *The Columbian*.

Cowlitz Valley District Ranger decisions: *The Chronicle*.

Malheur National Forest

Malheur Forest Supervisor, Blue Mountain District Ranger, and Prairie City District Ranger decisions: *Blue Mountain Eagle*.

Emigrant Creek District Ranger decisions: *Burns Times Herald*.

Mt. Baker-Snoqualmie National Forest

Mt. Baker-Snoqualmie Forest Supervisor, Darrington District Ranger, and Skykomish District Ranger decisions: *Everett Herald*.

Mt. Baker District Ranger decisions that encompass the southern half of the district: *Skagit Valley Herald*.

Mt. Baker District Ranger decisions that encompass the northern half of the district: *Bellingham Herald*.

Snoqualmie District Ranger decisions that encompass the northern half of the district: *Snoqualmie Valley Record*.

Snoqualmie District Ranger decisions that encompass the southern half of the district: *Enumclaw Courier Herald*.

Mt. Hood National Forest

Mt. Hood Forest Supervisor and District Ranger decisions: *The Oregonian*.

Ochoco National Forest and Crooked River National Grassland

Ochoco Forest Supervisor and District Ranger decisions: *The Bulletin*.

Okanogan-Wenatchee National Forest

Okanogan-Wenatchee Forest Supervisor, Chelan District Ranger, Entiat, and Wenatchee River District Ranger decisions: *The Wenatchee World*.

Naches District Ranger decisions: *Yakima Herald*.

Methow Valley District Ranger decisions: *Methow Valley News*.

Cle-Elum District Ranger decisions: *Ellensburg Daily Record*.

Olympic National Forest

Olympic Forest Supervisor and District Ranger decisions: *The Olympian*.

Rogue River-Siskiyou National Forest

Rogue River-Siskiyou Forest Supervisor, High Cascades District Ranger, J. Herbert Stone Nursery Manager, and Siskiyou Mountains District Ranger decisions: *Rogue Valley Times*.

Wild Rivers District Ranger decisions: *Grants Pass Daily Courier*.

Powers District Ranger decisions: *The World*.

Siuslaw National Forest

Siuslaw Forest Supervisor decisions: *Corvallis Gazette-Times*.

Central Coast Ranger District Ranger and Oregon Dunes National Recreation Area District Ranger decisions: *The Register-Guard*.

Hebo District Ranger decisions: *Tillamook Headlight Herald*.

Umatilla National Forest

Umatilla Forest Supervisor and District Ranger decisions: *East Oregonian*.

Umpqua National Forest

Umpqua Forest Supervisor and District Ranger decisions: *The News-Review*.

Wallowa-Whitman National Forest

Wallowa-Whitman Forest Supervisor and Whitman District Ranger decisions: *Baker City Herald*.

La Grande District Ranger decisions: *The Observer*.

Hells Canyon National Recreation Area Manager, Eagle Cap District Ranger, and Wallowa Valley District Ranger decisions: *Wallowa County Chieftain*.

Willamette National Forest

Willamette Forest Supervisor, Middle Fork District Ranger, McKenzie River District Ranger, and Sweet Home District Ranger decisions: *The Register-Guard*.

Detroit District Ranger decisions: *Statesman Journal*.

Dated: March 29, 2024.

Troy Heithecker,

Associate Deputy Chief, National Forest System.

[FR Doc. 2024-07120 Filed 4-3-24; 8:45 am]

BILLING CODE 3411-15-P

DEPARTMENT OF AGRICULTURE**Rural Business-Cooperative Service**

[Docket No: RBS-24-CO-OP-0003]

Notice of Funding Opportunity for Rural Cooperative Development Grants for Fiscal Year 2024

AGENCY: Rural Business-Cooperative Service, USDA.

ACTION: Notice.

SUMMARY: The Rural Business-Cooperative Service (RBCS or the Agency), a Rural Development (RD) agency of the United States Department of Agriculture (USDA), invites applications for grants under the Rural Cooperative Development Grant (RCDG) program for fiscal year (FY) 2024. This notice is being issued to allow applicants sufficient time to leverage financing, prepare and submit applications, and give the Agency time to process applications within FY 2024. Successful applications will be selected by the Agency for funding and subsequently awarded. All applicants are responsible for any expenses incurred in developing their applications.

DATES: Completed applications must be submitted electronically by no later than 11:59 p.m. eastern time (ET), June 3, 2024, through www.grants.gov, to be eligible for grant funding. Late or incomplete applications are not eligible for funding under this notice and will not be evaluated.

ADDRESSES: All applications must be submitted electronically at www.grants.gov. Additional resources are available at <https://www.rd.usda.gov/programs-services/business-programs/rural-cooperative->

development-grant-program, www.rd.usda.gov/programs-services/rural-cooperative-development-grant-program.

Applicants are encouraged to contact the USDA RD State Office for the State where the Project will be located in advance of the application deadline to discuss the Project and ask any questions about the RCDG program or the application process. Contact information for USDA RD State Offices can be found at www.rd.usda.gov/about-rd/offices/state-offices.

FOR FURTHER INFORMATION CONTACT: Lisa Sharp at lisa.sharp@usda.gov, Business Loan and Grant Analyst, Program Management Division, RBCS, USDA, 1400 Independence Avenue SW, Mail Stop-3226, Room 5160-South, Washington, DC 20250-3226, or call (202) 720-1400.

SUPPLEMENTARY INFORMATION:

Overview

Federal Awarding Agency Name: Rural Business-Cooperative Service.

Funding Opportunity Title: Rural Cooperative Development Grant.

Announcement Type: Notice of Funding Opportunity.

Funding Opportunity Number: RBCS-RCDG-2024.

Assistance Listing Number: 10.771.

Dates: Completed applications must be submitted electronically by 11:59 p.m. ET on, June 3, 2024, through www.grants.gov, to be eligible for grant funding. Late or incomplete applications are not eligible for funding under this notice and will not be evaluated.

Rural Development Key Priorities: The Agency encourages applicants to consider Projects that will advance the following key priorities (more details available at www.rd.usda.gov/priority-points):

- Creating More and Better Market Opportunities; Assisting Rural communities recover economically through more and better market opportunities and through improved infrastructure;
- Advancing Racial Justice, Place-Based Equity, and Opportunity; Ensuring all Rural residents have equitable access to RD programs and benefits from RD funded projects; and
- Addressing Climate Change and Environmental Justice; Reducing climate pollution and increasing resilience to the impacts of climate change through economic support to Rural communities.

A. Program Description

1. *Purpose of the Program.* The primary objective of the RCDG program

is to improve the economic condition of Rural Areas by helping individuals and businesses start, expand, or improve Rural cooperatives and Mutually Owned Businesses through Cooperative Development Centers.

2. *Statutory and Regulatory Authority.* The RCDG program is authorized under Section 310B(e) of the Consolidated Farm and Rural Development Act (CONACT) (7 U.S.C. 1932(e)), as amended by the Agriculture Improvement Act of 2018 (Pub. L. 115-334, title VI, secs. 6412-15, 6601(a)(1)(B), 6701(c), (d)(1)), and implemented by 7 CFR part 4284, subparts A and F.

The Consolidated Appropriations Act, 2024, (Pub. L. 118-42, Division B, title VII, sec. 736, has designated funding for Projects in Persistent Poverty Counties. Persistent poverty counties are defined in section 736 as “any county that has had 20 percent or more of its population living in poverty over the past 30 years, as measured by the 1990 and 2000 decennial censuses, and 2007–2011 American Community Survey 5-year average, or any territory or possession of the United States.” The eligible population in persistent poverty counties includes any county seat of any persistent poverty county that has a population that does not exceed the authorized population limit by more than 10 percent. This provision expanded the current 50,000 population limit to 55,000 for only county seats located in persistent poverty counties.

3. *Definitions.* The following definition, in addition to the ones published at 7 CFR 4284.3 and 4284.504, is applicable to this notice. In addition, the terms “Rural” and “Rural Area,” as defined in 7 U.S.C. 1991(a)(13), will be used for this program instead of the definition of “Rural and Rural Area” currently published at 7 CFR 4284.3. The first letter of each word in a defined term is capitalized from this point forward in the notice for easy identification.

Mutually Owned Business—An organization owned and governed by members who are its consumers, producers, employees, or suppliers.

4. *Application of Awards.* The Agency will review, evaluate, and score applications received in response to this notice based on the provisions found in 7 CFR 4284.511, .512, .513, and as indicated in this notice. Awards under the RCDG program will be made on a competitive basis using specific selection criteria contained in 7 CFR 4284.513.

B. Federal Award Information

Type of Award: Grant.

Fiscal Year Funds: FY 2024.

Available Funds: \$5.8 million will be available for FY 2024. RBCS may at its discretion, increase the total level of funding available in this funding round from any available source provided the awards meet the requirements of the statute which made the funding available to the Agency.

Award Amounts: Maximum amount \$200,000.

Anticipated Award Date: September 30, 2024.

Performance Period: The grant performance period should begin no earlier than October 1, 2024, and no later than January 1, 2025. The application must include no more than a one-year grant performance period, or it will not be considered for funding. Applications that request funds for a period beginning after January 1, 2025, will not be considered for funding. Projects must be completed within a one-year timeframe. Prior written approval is needed from the Agency if the applicant is awarded a grant and desires the grant performance period to begin earlier or later than previously approved.

Renewal or Supplemental Awards: None.

Type of Assistance Instrument: Financial Assistance Agreement.

C. Eligibility Information

1. *Eligible Applicants.* Eligible applicants must meet the eligibility requirements of 7 CFR 4284.507. You must be a nonprofit corporation or an institution of higher education to apply for this program. Public bodies and individuals are not eligible to apply for this program. Applicants must be aware of the following:

(a) At the time of application, each applicant must have an active registration in the System for Award Management (SAM) before submitting its application in accordance with 2 CFR 25.200. To register in SAM, entities will be required to obtain a Unique Entity Identifier (UEI). Instructions for obtaining the UEI are available at sam.gov/content/entity-registration. Further information regarding SAM registration and the UEI can be found in this notice.

(b) Each applicant must certify that it has not been debarred or suspended or is otherwise excluded from or ineligible for participation in Federal assistance programs under Executive Order 12549, Debarment and Suspension. The Agency will check the Do Not Pay (DNP) system at the time of application and prior to funding any grant award to determine if the applicant has been debarred or suspended. Applicants are responsible

for resolving any issues that are reported in the DNP system and if issues are not resolved by deadlines found in this notice, the Agency may proceed to award funds to other eligible applicants. In addition, an applicant must be eligible in accordance with 7 CFR 4284.6 and will be required to certify as part of the application that it does not have an outstanding judgment against it.

(c) The Further Consolidated Appropriations Act, 2024, Public Law 118–47, Division B, title VII, sections 744 and 745 provide that any corporation that has been convicted of a felony criminal violation under any Federal law within the past 24 months or that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, is not eligible for financial assistance provided with funds appropriated by this Act, unless a Federal agency has considered suspension or debarment of the corporation and has made a determination that this further action is not necessary to protect the interests of the Government.

2. *Cost Sharing or Matching.* A match of at least 25 percent (5 percent for 1994 Institutions) of the total project cost is required for the application as provided in 7 CFR 4284.513(f). When calculating the Matching Funds requirement, round up or down to whole dollars as appropriate.

An example of how to calculate Matching Funds is as follows:

(a) Take the amount of grant funds requested and divide it by .75. This will provide the total project cost.

Example: \$200,000 (grant amount)/0.75 (percentage for use of grant funds) = \$266,667 (total project cost)

(b) Subtract the amount of grant funds requested from the total project cost. This will provide the Matching Funds requirement.

Example: \$266,667 (total project cost) – \$200,000 (grant amount) = \$66,667 (Matching Funds requirement)

(c) A quick way to confirm the correct amount of Matching Funds is to take the total project cost and multiply it by .25.

Example: \$266,667 (total project cost) × .25 (maximum percentage of Matching Funds requirement) = \$66,667 (Matching Funds requirement)

The applicant must verify that all Matching Funds are available during the

grant performance period and provide documentation with the application in accordance with requirements identified in section D.2(b)(8) of this notice. If awarded a grant, additional verification documentation may be required to confirm the availability of Matching Funds.

Other rules for Matching Funds that applicants must follow are listed below.

(a) They must be spent on eligible expenses during the grant period.

(b) They must be from eligible sources.

(c) They must be spent in advance or as a pro-rata portion of grant funds being spent.

(d) They must be provided by either the applicant or a third party in the form of cash or an in-kind contribution.

(e) They cannot include board/advisory council member's time.

(f) They cannot include other Federal grants unless provided by authorizing legislation.

(g) They cannot include cash or in-kind contributions donated outside of the grant period.

(h) They cannot include over-valued, in-kind contributions.

(i) They cannot include any project costs that are ineligible under the RCDG program.

(j) They cannot include any project costs that are restricted or unallowable under 2 CFR part 200, subpart E, and the Federal Acquisition Regulation (CFR title 48) (for-profits) or successor regulation.

(k) They can include loan funds from a Federal source.

(l) They can include travel and incidentals for board/advisory council members if the organization has established written policies explaining how these costs are normally reimbursed, including rates. The applicant must include an explanation of this policy in the application, or the contributions will not be considered as eligible Matching Funds.

(m) The applicant must be able to document and verify the number of hours worked and the value associated with any in-kind contribution being used to meet a Matching Funds requirement.

(n) In-kind contributions provided by individuals, businesses, or cooperatives which are being assisted by the applicant cannot be provided for the direct benefit of their own projects as RD considers this to be a Conflict of Interest or the appearance of a Conflict of Interest.

3. *Other Eligibility Requirements.*

(a) *Purpose eligibility.* Applications must propose the establishment or continuation of a Cooperative

Development Center. Applicants must use project funds, including grant and Matching Funds, for eligible purposes only (see 7 CFR 4284.508). In addition, project funds may also be used for programs providing for the coordination of services and sharing of information among the Centers as stated in 7 U.S.C. 1932(e)(4)(C)(vi).

(b) *Project eligibility.* All Project activities must be for the benefit of a Rural Area.

(c) *Multiple applications deemed ineligible.* Only one application can be submitted per applicant. If two applications are submitted (regardless of the applicant's name) that include the same Executive Director and/or advisory boards or committees of an existing Center, both applications will be determined ineligible for funding.

(d) *Satisfactory performance.* Applicants must be performing satisfactorily on any outstanding RCDG award to be considered eligible for a new award. Satisfactory performance includes being up to date on all financial and performance reports as prescribed in the grant award, and current on all tasks and timeframes for utilizing grant and Matching Funds as approved in the work plan and budget. If applicants have any unspent grant funds on RCDG awards prior to FY 2023, the application will not be considered for funding. If an applicant has prior award(s) with unspent funds of 50 percent or more than what the approved work plan and budget projected at the time a FY 2024 application is being evaluated, the application will not be considered for funding. The Agency will verify the performance status of the applicant's prior awards and make a determination after the FY 2024 application period closes.

(e) *Duplication of current services.* Applications must demonstrate that the applicant is providing services to new customers or new services to current customers. If the work plan and budget are duplicative of the applicant's existing award, the application will not be considered for funding. If the workplan and budget are duplicative of a previous or existing RCDG and/or Socially Disadvantaged Groups Grant award, the application will not be considered for funding. The Agency will make this determination at its sole discretion. Please note that the Agency only allows one active RCDG award to a grantee to ensure that there is no duplication of services.

(f) *Indirect costs.* Negotiated indirect cost rate approval does not need to be included in the application but will need to be provided if a grant is

awarded. Approval for indirect costs that are requested in an application without an approved indirect cost rate agreement is at the discretion of the Agency. Applicants considering a de minimis rate or in need of establishing an indirect cost rate should discuss these options with the Agency.

D. Application and Submission Information

1. *Address to Request Application Package.* The RCDG program application template, copies of necessary forms and samples are available at www.rd.usda.gov/programs-services/rural-cooperative-development-grant-program. The RCDG program regulations are available at 7 CFR part 4284 subparts A and F. For further information, contact the USDA State Office where the Project will be located at www.rd.usda.gov/contact-us/state-offices.

2. *Content and Form of Application Submission.* An application must contain all the required elements outlined in 7 CFR 4284.510 and this notice. Each application must address the applicable scoring criteria presented in 7 CFR 4284.513 and this notice for the type of funding being requested.

Applicants are encouraged, but not required, to utilize the application template found at www.rd.usda.gov/programs-services/rural-cooperative-development-grant-program. The application template provides specific, detailed instructions for each item of a complete application. The Agency emphasizes the importance of including every item and strongly encourages applicants to follow the instructions carefully, using the examples and illustrations in the application template.

Incomplete applications will be ineligible to compete for funds. Applications lacking sufficient information to determine eligibility and scoring will be considered ineligible. Information submitted after the application deadline will not be accepted.

(a) Clarifications on Forms.

(1) *Form SF-424, "Application for Federal Assistance."* This form must include the applicant's Unique Entity Identifier (UEI) number in item 8c on the form. The UEI is assigned automatically to all active *SAM.gov* registered entities. If an applicant does not include the UEI number in the application, it will not be considered for funding.

(2) *Form SF 424B, Assurances—Non-Construction Programs.* This form is no longer required as a part of the application. This information is now collected through the applicant's

registration or annual recertification in *SAM.gov* through the Financial Assistance General Representations and Certifications.

(b) *Clarifications on Proposal Elements.* Requirements below are provided in addition to the requirements provided in 7 CFR 4284.510(c).

(1) *Title Page.* Must include the title of the Project as well as any other relevant identifying information.

(2) *Table of Contents.* This must include page numbers for each component of the application.

(3) *Executive Summary.* In addition to the items in 7 CFR 4284.510(c)(3), this must discuss the percentage of work that will be performed among organizational staff, consultants, or other contractors. The summary must not exceed two pages.

(4) *Eligibility.* This discussion must also include Matching Funds and other eligibility requirements. This discussion must not exceed two pages.

(5) *Proposal Narrative.* Must not exceed 40 pages using at least 11-point font and should describe the essential aspects of the Project. The Executive Summary and Eligibility discussion are not included within the 40-page limit of the proposal narrative.

(i) *Information Sheet.* If evaluation criteria are listed on the Table of Contents and then specifically and individually addressed in narrative form, it is not necessary to include an information sheet. Otherwise, it is required as described at 7 CFR 4284.510(c)(5)(ii).

(ii) Goals of the Project.

(A) Applicant must include a statement providing information outlined in 7 CFR 4284.510(c)(5)(iii)(A), (B), (C) and (D).

(B) Expected economic impacts should be tied to tasks included in the work plan and budget.

(iii) *Performance Evaluation Criteria.* The Agency has established annual performance evaluation measures to evaluate the RCDG program and the applicant must provide estimates on the following:

(A) Number of groups assisted who are not legal entities.

(B) Number of businesses assisted that are not cooperatives.

(C) Number of cooperatives assisted.

(D) Number of businesses incorporated that are not cooperatives.

(E) Number of cooperatives incorporated.

(F) Total number of jobs created as a result of assistance.

(G) Total number of jobs saved as a result of assistance.

(H) Number of jobs created for the Center as a result of RCDG funding.

(I) Number of jobs saved for the Center as a result of RCDG funding.

It is permissible to have a zero in a performance element. When calculating jobs created, estimates should be based upon actual jobs to be created by the organization because of the RCDG funding or actual jobs to be created by cooperative businesses or other businesses as a result of assistance from the organization. When calculating jobs saved, estimates should be based only on actual jobs that would have been lost if the organization did not receive RCDG funding or actual jobs that would have been lost without assistance from the organization.

Additional performance elements may be included. In instances where job creation or job retention may not be a relevant indicator, applicants should provide relevant, specific and measurable performance elements that could be included in an award document. For example, applicants may consider the following as it relates to their specific work: housing cooperatives (number of units created or preserved); worker cooperatives (number of jobs created, number of employee-owned positions created); consumer cooperatives (number of people with access to groceries, renewable energy services); shared services cooperatives (number of businesses with access to affordable products or services, joint marketing, distribution channels); real estate cooperatives (number of community members invested in their community, number of real estate properties created or saved).

(iv) *Undertakings.* The applicant must expressly undertake to do the following:

(A) Take all practicable steps to develop continuing sources of financial support for the Center, particularly from sources in the private sector;

(B) Make arrangements for the activities by the Nonprofit Institution operating the Center to be monitored and evaluated; and

(C) Provide an accounting for the money received by the grantee under this subpart.

(v) *Work Plan.* Work plan and budget proposal elements should be addressed under proposal narrative criterion in 7 CFR 4284.510(c)(5)(iv), utilizing the specific requirements of Section E.1(h) of this notice.

(vi) *Delivery of Cooperative Development Assistance.* The applicant must describe its previous accomplishments and outcomes in Cooperative Development activities and/or its potential for effective delivery of Cooperative Development services to Rural Areas. The description(s) should

be addressed under proposal narrative criterion in 7 CFR 4284.510(c)(5)(vii) utilizing the specific requirements of technical assistance and other services in Section E.1(b) of this notice.

(vii) *Qualifications of Personnel.*

Applicants must describe the qualifications of personnel expected to perform key Center tasks, and whether these personnel are to be full/part-time Center employees or contract personnel. All requirements of 7 CFR 4284.510(c)(5)(viii) should be addressed under the proposal narrative criterion, utilizing the specific requirements of qualifications of those performing the tasks in Section E.1(i) of this notice.

(viii) *Support and Commitments and Future Support.* Applicants must describe the level of support and commitment in the community for the proposed Center and the services it would provide under 7 CFR 4284.510(c)(5)(ix) and the future support and funding under 7 CFR 4284.510(c)(5)(x) utilizing the requirements of commitment in section E.1(f) and local and future support in section E.1(j) of this notice.

(ix) *Proposal Evaluation Criteria.*

Applications will not be considered for funding if they do not address all of the proposal evaluation criteria. See application review information in Section E.1. of this notice for a description of the proposal evaluation criteria.

(x) *Relevant Information.* Only appendices A–C will be considered when evaluating applications. Do not include resumes of staff or consultants in the application.

(6) *No Current Outstanding Federal Judgments Certification.* Each applicant must certify that the United States has not obtained an unsatisfied judgement against its property, is not delinquent on the payment of federal income taxes or any other federal debt and will not use grant funds to pay judgments obtained by the United States. Applicants should make this certification within their application with this statement in the application: “[INSERT NAME OF APPLICANT] certifies that the United States has not obtained an unsatisfied judgment against its property, is not delinquent on the payment of Federal income taxes, or any Federal debt, and will not use grant funds to pay any judgments obtained by the United States.” A separate signature relating to this certification is not required.

(7) *Certification.* Applicants must certify that they have obtained Matching Funds as required by 7 CFR 4284.510(c)(7). Applicants should make this certification within their certification, with this statement:

“[INSERT NAME OF APPLICANT] certifies that Matching Funds will be available at the same time grant funds are anticipated to be spent and that expenditures of Matching Funds shall be pro-rated or spent in advance of grant funding, such that for every dollar of the total project cost, at least 25 cents (5 cents for 1994 Institutions) of Matching Funds will be expended.” A separate signature relating to this certification is not required.

(8) *Verification of Matching Funds.*

Applicants must verify all Matching Funds. The documentation must be included in Appendix A of the application and will not count towards the 40-page limitation. The Agency recommends making this verification with a template letter, but the template is not required. Template letters are available for each type of Matching Funds contribution at: www.rd.usda.gov/programs-services/rural-cooperative-development-grant-program.

(i) *Matching Funds provided in cash.* The following requirements must be met:

(A) *Provided by the Applicant.* The application must include a statement verifying: (1) the amount of the cash and (2) the source of the cash. Applicants may also provide a bank statement dated 30 days or less from the application deadline date to verify a cash match.

(B) *Provided by a Third-Party.* The application must include a signed letter from the third party verifying: (1) how much cash will be donated and (2) that it will be available corresponding to the proposed time frame or donated on a specific date within the grant performance period.

(ii) *Matching Funds provided by an in-kind donation.* The following requirements must be met:

(A) *Provided by the Applicant.* The application must include a signed letter from the applicant or the authorized representative verifying: (1) the nature of the goods and/or services to be donated and how they will be used, (2) when the goods and/or services will be donated (*i.e.*, corresponding to the proposed grant performance period or to specific dates within the specified time frame), and (3) the value of the goods and/or services. Please note that most applicant contributions for the RCDG program are considered applicant cash match in accordance with this notice. Applicants needing clarification for verification of Matching Funds should contact the RD State Office. Identifying Matching Funds improperly can affect application scoring.

(B) *Provided by a Third-Party.* The application must include a signed letter from the third party verifying: (1) the nature of the goods and/or services to be donated and how they will be used, (2) when the goods and/or services will be donated (*i.e.*, corresponding to the proposed grant performance period or to specific dates within the grant performance period), and (3) the value of the goods and/or services.

(iii) *Identification and Verification of Matching Funds.* To ensure applicants are identifying and verifying Matching Funds appropriately, please note the following:

(A) If applicants are paying for goods and/or services as part of the Matching Funds requirement, the expenditure is considered a cash match, and must verify it as such. Universities must verify the goods and services they are providing to the Project as a cash match and the verification must be approved by the appropriate approval official (*i.e.*, sponsored programs office or equivalent).

(B) If applicants have already received cash from a third party (*e.g.*, a foundation) before the start of the proposed grant performance period, the applicant must verify this as its own cash match and not as a third-party cash match. If applicants are receiving cash from a third party during the grant performance period, then the applicant must verify the cash as a third-party cash match.

(C) Board resolutions for a cash match must be approved at the time of application.

(D) Applicants can only consider goods or services for which no expenditure is made as an in-kind contribution.

(E) If a non-profit or another organization contributes the services of affiliated volunteers, they must follow the third-party, in-kind donation verification requirement for each individual volunteer.

(F) Expected program income may not be used to fulfill the applicant Matching Funds requirement at the time of the application submission. If the applicant has a contract to provide services in place at the time of application submission, then they must submit the contract with the application, and applicants can verify the amount of the contract as a cash match.

(G) The valuation processes used for in-kind contributions do not need to be included in the application, but applicants must be able to demonstrate how the valuation was derived if a grant is awarded. The grant award may be withdrawn, or the amount of the grant

reduced if applicant cannot demonstrate how the valuation was derived.

Successful applicants must comply with requirements identified in this notice in Section F, Federal Award Administration Information.

(c) *Completeness.* An application will not be considered for funding if it fails to meet all eligibility criteria by the application deadline or does not provide sufficient information to determine eligibility and scoring. Applicants must include, in one submission to the Agency, all the forms and proposal elements as discussed in the program regulation and as clarified further in this notice. Incomplete applications will not be reviewed by the Agency.

3. System for Award Management and Unique Entity Identifier.

(a) At the time of application, each applicant must have an active registration in the SAM before submitting its application in accordance with 2 CFR part 25. To register in SAM, entities will be required to obtain a UEI. Instructions for obtaining the UEI are available at sam.gov/content/entity-registration.

(b) Each applicant must maintain an active SAM registration, with current, accurate and complete information, at all times during which it has an active Federal award or an application under consideration by a Federal awarding agency.

(c) Each applicant must ensure that it completes the Financial Assistance General Representations and Certifications in SAM.

(d) Each applicant must provide a valid UEI in its application, unless determined exempt under 2 CFR 25.110.

(e) The Agency will not make an award until the applicant has complied with all SAM requirements including providing the UEI. If an applicant has not fully complied with the requirements by the time the Agency is ready to make an award, the Agency may determine that the applicant is not qualified to receive a Federal award and use that determination as a basis for making a Federal award to another applicant.

4. Submission Dates and Times.

(a) *Application Technical Assistance.* Prior to official submission of applications, applicants may request technical assistance or other application guidance from the Agency, if such requests are made prior to May 6, 2024. Agency contact information can be found in Section G of this notice.

(b) *Application Deadline Date.* Completed applications must be submitted electronically through www.grants.gov and received no later

than 11:59 p.m. ET on June 3, 2024, to be eligible for grant funding. Please review the [Grants.gov](https://www.grants.gov) website at www.grants.gov/register for instructions on the process of registering an organization as soon as possible to ensure that all electronic application deadlines are met. *Grants.gov* will not accept applications submitted after the deadline.

The Agency will not solicit or consider new scoring or eligibility information that is submitted after the application deadline. RBCS also reserves the right to ask applicants for clarifying information and additional verification of assertions in the application.

5. *Intergovernmental Review.* Executive Order (E.O.) 12372, Intergovernmental Review of Federal Programs, applies to this program. This E.O. requires that Federal agencies provide opportunities for consultation on proposed assistance with State and local governments. Many States have established a Single Point of Contact (SPOC) to facilitate this consultation. For a list of States that maintain a SPOC, please see the White House website: www.whitehouse.gov/omb/office-federal-financial-management/. If the applicant's State has a SPOC, then a copy of the application must be submitted for review. Any comments obtained through the SPOC must be provided to the applicant's State Office for consideration as part of the application. If the applicant's State has not established a SPOC, applications may be submitted directly to the Agency. Applications from federally recognized Indian Tribes are not subject to this requirement.

6. Funding Restrictions.

(a) The use of grant funds is outlined at 7 CFR 4284.508. Grant funds may be used to pay for up to 75 percent of the cost of establishing and operating centers for Rural Cooperative Development. Grant funds may be used to pay for 95 percent of the cost of establishing and operating centers for Rural Cooperative Development when the applicant is a college identified as a "1994 Institution" for purposes of the Equity in Educational Land-Grant Status Act of 1994, as defined by 7 U.S.C. 301 note; Public Law 103-382, as amended.

(b) As required by 7 U.S.C. Chapter 38, Subchapter VII and 7 CFR part 990, no assistance or funding can be provided to a hemp producer unless they have a valid license issued from an approved State, Tribal or Federal plan as defined by 7 U.S.C. 1639o. Verification of valid hemp licenses will occur at the time of award. The purpose of the RCDG program is to provide

technical assistance, so funding to produce hemp or marketing hemp production is not eligible.

(c) Project funds, including grant and Matching Funds, cannot be used for ineligible grant purposes as provided in 7 CFR 4284.10. Also, applicants shall not use Project funds for the following:

(1) To purchase, rent, or install laboratory equipment or processing machinery;

(2) To pay for the operating costs of any entity receiving assistance from the Center;

(3) To pay costs of the Project where a Conflict of Interest exists;

(4) To fund any activities prohibited by 2 CFR part 200; or

(5) To fund any activities considered unallowable by 2 CFR part 200, subpart E, Cost Principles, and the Federal Acquisition Regulation or successor regulations.

(d) In addition, an application will not be considered for funding if it does any of the following:

(1) Focuses assistance on only one cooperative or Mutually Owned Business;

(2) Requests more than the maximum grant amount; or

(3) Proposes ineligible costs that equal more than 10 percent of total project costs. The ineligible costs will NOT be removed at this stage to proceed with application processing. For purposes of this determination, the grant amount requested plus the Matching Funds amount constitutes the total project costs.

(e) We will consider applications for funding that include ineligible costs of 10 percent or less of total project costs if the remaining costs are determined eligible. If the application is successful, ineligible costs must be removed and replaced with eligible costs before the Agency makes the grant award, or the amount of the grant award will be reduced accordingly. If the Agency cannot determine the percentage of ineligible costs due to lack of detail, the application will not be considered for funding.

7. *Other Submission Requirements.* Applications must be submitted electronically. Note that we cannot accept applications submitted through mail or courier delivery, in-person delivery, email, or fax. For electronic applications, applicants must follow the instruction for this funding announcement at www.grants.gov. Applicants can locate the *Grants.gov* downloadable application package for this program by using a keyword, the program name, Assistance Listing Number or the Funding Opportunity Number for this program.

Users of *Grants.gov* must already have a UEI number and must also be registered and maintain registration in SAM in accordance with 2 CFR part 25. The UEI number must be associated with the correct tax identification number of the RCDG applicant. We strongly recommend that applicants do not wait until the application deadline date to begin the application process through *Grants.gov*.

All application documents must be submitted through *Grants.gov*. Applications must include electronic signatures. Original signatures may be required if funds are awarded. After electronically applying through *Grants.gov*, applicants will receive an automated acknowledgement from *Grants.gov* that contains a *Grants.gov* tracking number.

E. Application Review Information

1. *Criteria*. Scoring criteria will follow statutory criteria in 7 U.S.C. 1932(e), the criteria published in the program regulations at 7 CFR 4284.513, and criteria in this notice. Applicants should also include Content and Form of Application Submission information as described in Section D.2 of this notice, if addressing these items under the scoring criteria. Evaluators will base scores only on the responses within each individual scoring criteria. Applicant may cross-reference another section to avoid duplication of narrative. The maximum number of points available is 110. Newly established or proposed Centers that do not yet have a track record on which to evaluate the criteria should refer to the expertise and track records of staff or consultants expected to perform tasks related to the respective criteria. Proposed or newly established Centers must be organized well enough at the time of application to address their capabilities for meeting these criteria.

The clarifications provided below are in addition to, and do not replace the guidance provided in 7 CFR 4284.513.

(a) *Administrative Capabilities*. Maximum score of ten (10) points. At a minimum, applicants must discuss the administrative capabilities provided in 7 CFR 4284.513(a) and expertise in administering Federal grant funding within the last five years, including but not limited to past RCDG awards. Please list the name of the Federal grant program(s), the amount(s), and the date(s) of funding received.

Applicants will score higher on this criterion by demonstrating that the Center has independent governance. Applicants that are universities or parent organizations should

demonstrate that there is a separate board of directors for the Center.

(b) *Technical Assistance and Other Services*. Maximum score of ten (10) points. Each application will be evaluated based on its demonstrate expertise within the last five years in providing technical assistance and accomplishing effective outcomes in Rural Areas to promote and assist the development of cooperatively and Mutually Owned Businesses. At a minimum, applicants must discuss:

- (1) Potential for delivering effective technical assistance;
- (2) The types of assistance provided;
- (3) The expected effects of that assistance;
- (4) The sustainability of organizations receiving the assistance; and
- (5) The transferability of the applicant's Cooperative Development strategies and focus to other areas of the United States.

A chart or table showing the outcomes of the demonstrated expertise based upon the performance elements listed in Section D.2(b)(5)(iii) of this notice or as identified in the award document on previous RCDG awards is recommended. At a minimum, please provide information for FY 2019 to FY 2023 awards. Applicants may also include any performance outcomes from a FY 2023 RCDG award. It is preferred that one chart or table for each award year be provided. The intention is for the applicant to provide actual performance numbers based upon award years (fiscal year) even though the grant performance period for the award was implemented during the next calendar or fiscal year. If applicants have not previously received an RCDG award, provide a narrative of explanation.

Applicants will score higher on this criterion by providing evidence of outcomes for more than three fiscal year awards and demonstrating that any organizations assisted within the last five years are sustainable. Please describe specific Project(s) when addressing items 1–5 of paragraph (b) of this section. To reduce duplication, descriptions of specific Projects and their impacts, outcomes, and roles can be discussed once under criterion (b) or (c) of this section. Applicants must cross-reference the information under the other criterion.

(c) *Economic Development*. Maximum score of ten (10) points. Applicant's demonstrated ability to assist in the development of the items listed in 7 CFR 4284.513(c) or Mutually Owned Businesses will be evaluated. Examples of facilitating development of new cooperative approaches are organizing

cooperatives among underserved individuals or communities; an innovative market approach; a type of cooperative currently not in the applicant's service area; a new cooperative structure; novel ways to raise member equity or community capitalization; conversion of an existing business to cooperative ownership.

Applicants will score higher on the Economic Development criteria by providing quantifiable economic measurements showing the impacts of past development projects within the last five years, and details of the applicant's role in Economic Development outcomes.

(d) *Past performance in Establishing Legal Business Entities*. Maximum score of ten (10) points. Applicants demonstrating past performance in establishing legal cooperative business entities and other legal business entities since October 1, 2019, will be evaluated. Provide the name of the organization(s) established, the date(s) of formation, and the applicant's role(s) in assisting with the incorporation(s) under this criterion. Documentation verifying the establishment of legal business entities must be included in Appendix C of the application and will not count against the 40-page limit for the narrative. The documentation must include proof that organizational documents were filed with the Secretary of State's Office (*i.e.*, Certificate of Incorporation or information from the State's official website naming the entity established and the date of establishment); or if the business entity is not required to register with the Secretary of State, or a certification from the business entity that a legal business entity has been established and when. Please note that applicants are not required to submit articles of incorporation to receive points under this criterion. Applicants that are an established legal cooperative business will score higher on this criterion. If the applicant's State does not incorporate cooperative business entities, please describe how the established business entity operates like a cooperative. Examples may include, but are not limited to, principles and practices of shared ownership, democratic control, and distribution of net income based on use of the business rather than equity contributed.

(e) *Networking and Regional Focus*. Maximum score of ten (10) points. A panel of USDA employees will evaluate the applicant's demonstrated commitment to:

- (1) Networking with other Cooperative Development Centers, and other organizations involved in Rural Economic Development efforts, and

(2) Developing multi-organizational and multi-State approaches to addressing the Economic Development and cooperative needs of Rural Areas.

Applicants will score higher on this criterion by demonstrating the outcomes of multi-organizational and multi-State approaches. Please describe the Project(s), partners and the outcome(s) that resulted from the approach.

(f) *Commitment*. Maximum score of ten (10) points. See 7 CFR 4284.513(e). Applicants will score higher on this criterion by defining and describing the underserved and economically distressed areas within the service area, provide economic statistics, and identify past or current Projects within or affecting these areas, as appropriate. Persistent poverty counties provisions are included in the 2024 Consolidated Appropriations Act, therefore Projects identified in the work plan and budget that are located in persistent poverty counties, will score higher on this criterion.

(g) *Matching Funds*. Maximum score of ten (10) points. Each applicant's Matching Funds requirements will be evaluated on requirements listed in 7 CFR 4284.513(f). A chart or table should be provided to describe all Matching Funds being committed to the Project. Formal documentation to verify all the Matching Funds must be included in Appendix A of the application. Applicants will be scored on the total amount and type of Matching Funds (cash vs. in-kind). You will be scored on the total amount and how you identify your Matching Funds.

(1) If you meet the 25 percent (5 percent for 1994 Institutions) Matching Funds requirement, points will be assigned as follows:

- (i) In-kind only—one (1) point;
- (ii) Mix of in-kind and cash—Three (3) to four (4) points (maximum points will be awarded if the ratio of cash to in-kind is 30 percent or more); or
- (iii) Cash only—five (5) points.

(2) If you exceed the 25 percent (5 percent for 1994 Institutions) Matching Funds requirement, points will be assigned as follows:

- (i) In-kind only—two (2) points;
- (ii) Mix of in-kind and cash—six (6) to seven (7) points (maximum points will be awarded if the ratio of cash to in-kind is 30 percent or more); or
- (iii) Cash only—up to ten (10) points.

(h) *Work Plan/Budget*. Maximum score of ten (10) points. Applicant's work plan will be evaluated for detailed actions and an accompanying timetable for implementing the proposal. The budget must present a breakdown of the estimated costs associated with cooperative and business development

activities as well as the operation of the Center and allocate these costs to each of the tasks to be undertaken. Matching Funds as well as grant funds must be accounted for separately in the budget. At a minimum, the following should be discussed.

(1) Specific tasks (whether it be by type of service or specific project) to be completed using grant and Matching Funds;

(2) How customers will be identified;

(3) Key personnel; and

(4) The evaluation methods to be used to determine the success of specific tasks and overall objectives of Center operations. Please provide qualitative methods of evaluation. For example, evaluation methods should go beyond quantitative measurements of completing surveys or number of evaluations.

Applicants will score higher on this criterion by presenting a clear, logical, realistic, and efficient work plan and budget.

(i) *Qualifications of those Performing the Tasks*. Maximum score of ten (10) points. The application will be evaluated to determine if the requirements of 7 CFR 4284.513(i) have been met. The application must indicate whether the personnel expected to perform the tasks are full/part-time employees of the organization or are contract personnel. Applicants will score higher on this criterion by demonstrating commitment and availability of qualified personnel expected to perform the tasks.

(j) *Local and Future Support*. Maximum score of ten (10) points. A panel of USDA employees will evaluate each application for local and future support. Support should be discussed directly when responding to this criterion.

(1) Discussion of local support should include previous and/or expected local support and plans for coordinating with other developmental organizations in the proposed service area, or with State and local government institutions. Applicants will score higher by demonstrating strong support from potential beneficiaries and formal evidence of intent to coordinate with other developmental organizations. Applicants may also submit a maximum of ten letters of support or intent to coordinate with the applicant to verify discussion of local support. These letters should be included in Appendix B of the application and will not count against the 40-page limit for the narrative. Documentation to verify local support will be required before an award is made.

(2) Discussion of future support is required in the applicant's vision for funding operations in future years. Applicants should document:

(i) New and existing funding sources that support applicant goals;

(ii) Alternative funding sources that reduce reliance on Federal, State, and local grants; and

(iii) The use of in-house personnel for providing services versus contracting out for expertise. Please discuss the strategy for building in-house technical assistance capacity.

Applicants will score higher by demonstrating that future support will result in long-term sustainability of the Center, including the fostering of in-house personnel development in order to provide services.

(k) *Administrator Discretionary Points*. Maximum score of ten (10) points. The Administrator may choose to award up to 10 points to an eligible non-profit corporation or institution of higher education that has never previously been awarded an RCDG grant or whose application seeks to advance the key priorities addressed in the Supplemental Section of this notice and detailed below. Points will be assigned as follows:

(1) Applicant has never received a RCDG award—five (5) points;

(2) Applicant seeks to advance one or more of the following key priorities—five (5) points:

(i) Assisting Rural communities recover economically through more and better market opportunities and through improved infrastructure. Applicant would receive priority points if the Project is located in or serving a Rural community whose economic well-being ranks in the most distressed tier (distress score of 80 or higher) of the Distressed Communities Index using the Distressed Communities Look-Up Map available at www.rd.usda.gov/priority-points.

(ii) Ensuring all Rural residents have equitable access to RD programs and benefits from RD funded projects. Using the Social Vulnerability Index (SVI) Look-Up Map (available at www.rd.usda.gov/priority-points), an applicant would receive priority points if the Project is: Located in or serving a community with a score 0.75 or above on the SVI;

- Is a federally recognized Tribe, including Tribal instrumentalities and entities that are wholly owned by Tribes; or
- Is a Project where at least 50 percent of the Project beneficiaries are members of federally Recognized Tribes and non-Tribal applicants include a Tribal Resolution of Consent from the

Tribe or Tribes that the applicant is proposing to serve.

(iii) Reducing climate pollution and increasing resilience to the impacts of climate change through economic support to Rural communities. Using the Disadvantaged Community and Energy Community Look-Up Map (available at www.rd.usda.gov/priority-points), applicants will receive priority in three ways:

- If the Project is located in or serves a Disadvantaged Community as defined by the Climate and Economic Justice Screening Tool (CEJST), from the White House Council on Environmental Quality;

- If the Project is located in or serves an Energy Community as defined by the Inflation Reduction Act (IRA); and
- If applicants can demonstrate through a written narrative how the proposed climate-impact Projects will improve the livelihoods of community residents and meet pollution mitigation or clean energy goals.

2. *Review and Selection Process.* The USDA RD State Office will review applications to determine if they are eligible for assistance based on requirements in 7 CFR part 4284, subparts A and F, this notice, and other applicable Federal regulations. If determined eligible, applications will be scored by a panel of USDA employees in accordance with the point allocation specified in section E.1 of this notice. The Administrator may choose to award up to ten (10) Administrator priority points based on criteria (k) in section E.1. of this notice. These points will be added to the cumulative score for a total possible score of 110. Applications will be funded in highest ranking order until the appropriations funding limitation for the RCDG program has been reached. Applications that cannot be fully funded may be offered partial funding at the Agency's discretion. The Agency reserves the right to offer the applicant less than the full amount of grant funding requested. Applications evaluated, but not funded, will not be carried forward into the competition for any subsequent fiscal year program funding. Successful applicants must comply with requirements identified in Section F of this notice.

F. Federal Award Administration Information

1. *Federal Award Notices.* If an application is selected for funding, the applicant will receive a signed notice of Federal award by postal or electronic mail from the USDA RD State Office where the applicant is located containing instructions and requirements necessary to proceed with

execution and performance of the award. Applicants must comply with all applicable statutes, regulations, and notice requirements before the grant award will be funded.

Applicants not selected for funding will be notified in writing via postal or electronic mail and informed of any review and appeal rights. See 7 CFR part 11 for USDA National Appeals Division (NAD) procedures. Note that rejected applicants that are successful in their NAD appeals will not receive funding if all FY 2024 RCDG program funding has already been awarded and obligated to other applicants.

2. *Administrative and National Policy Requirements.* Additional requirements that apply to grantees selected for this program can be found in 7 CFR part 4284, subpart F; the Grants and Agreements regulations applicable to the Department of Agriculture codified in 2 CFR parts 180, 200, 400, 415, 417, 418, 421; 2 CFR parts 25 and 170; and 48 CFR part 31, and successor regulations to these parts.

In addition, all recipients of Federal financial assistance are required to report information about first tier subawards and executive compensation in accordance with 2 CFR part 170. Applicants will be required to have the necessary processes and systems in place to comply with the Federal Funding Accountability and Transparency Act of 2006 (Pub. L. 109-282) reporting requirements (see 2 CFR 170.200(b)), unless exempt under 2 CFR 170.110(b)).

The following additional requirements apply to grantees selected for awards within this program:

(a) Execution of Form RD 4280-2, Rural Business Cooperative Service Financial Assistance Agreement;

(b) Acceptance of a written Letter of Conditions; and submission of the following Agency forms:

(1) Form RD 1940-1, Request for Obligation of Funds.

(2) Form RD 1942-46, Letter of Intent to Meet Conditions.

(3) SF LLL, Disclosure of Lobbying Activities, if applicable.

3. *Reporting.* After grant approval and through grant completion, applicants will be required to provide an SF-425, Federal Financial Report, and a Project performance report on a semiannual basis (due 30 working days after the end of the semiannual period). The Project performance reports shall include the following:

(a) A comparison of actual accomplishments to the objectives established for that period;

(b) Reasons why established objectives were not met, if applicable;

(c) Reasons for any problems, delays, or adverse conditions, if any, which have affected or will affect attainment of overall Project objectives, prevent meeting time schedules or objectives, or preclude the attainment of particular objectives during established time periods. This disclosure shall be accompanied by a statement of the action taken or planned to resolve the situation; and

(d) The grantee must provide a final Project and financial status report within 90 days after the expiration or termination of the grant performance period with a summary of the Project performance reports and final deliverables to close out a grant in accordance with 2 CFR 200.344.

G. Federal Awarding Agency Contact(s)

For general questions about this announcement, please contact the USDA RD State Office provided in the **ADDRESSES** section of this notice.

H. Other Information

1. *Paperwork Reduction Act.* In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. chapter 35), the information collection requirements associated with the program, as covered in this notice, have been approved by the Office of Management and Budget (OMB) under OMB Control Number 0570-0006.

2. *National Environmental Policy Act (NEPA).* All recipients under this notice are subject to the requirements of 7 CFR part 1970. However, awards for technical assistance and training under this notice are classified as a Categorical Exclusion pursuant to 7 CFR 1970.53(b), and usually do not require any additional documentation. RBCS will review each grant application to determine its compliance with 7 CFR part 1970. The applicant may be asked to provide additional information or documentation to assist RBCS with this determination. A review for NEPA compliance is required prior to the award of grant funds.

3. *Federal Funding Accountability and Transparency Act.* All applicants, in accordance with 2 CFR part 25, must be registered in SAM and have a UEI number as stated in Section D.3 of this notice. All recipients of Federal funding are required to report information about first-tier sub-awards and executive total compensation in accordance with 2 CFR part 170.

4. *Civil Rights Act.* All grants made under this notice are subject to Title VI of the Civil Rights Act of 1964 as required by the USDA (7 CFR part 15, subpart A and section 504 of the Rehabilitation Act of 1973, title VIII of

the Civil Rights Act of 1968, title IX, Executive Order 13166 (Limited English Proficiency), Executive Order 11246, and the Equal Credit Opportunity Act of 1974).

5. *Nondiscrimination Statement.* In accordance with Federal civil rights laws and USDA civil rights regulations and policies, the USDA, its Mission Areas, agencies, staff offices, employees, and institutions participating in or administering USDA programs are prohibited from discriminating based on race, color, national origin, religion, sex, gender identity (including gender expression), sexual orientation, disability, age, marital status, family/parental status, income derived from a public assistance program, political beliefs, or reprisal or retaliation for prior civil rights activity, in any program or activity conducted or funded by USDA (not all bases apply to all programs). Remedies and complaint filing deadlines vary by program or incident.

Program information may be made available in languages other than English. Persons with disabilities who require alternative means of communication to obtain program information (e.g., Braille, large print, audiotape, American Sign Language) should contact the responsible Mission Area, Agency, or staff office; or the 711 Relay Service.

To file a program discrimination complaint, a complainant should complete a Form AD-3027, USDA Program Discrimination Complaint Form, which can be obtained online at www.usda.gov/sites/default/files/documents/ad-3027.pdf, from any USDA office, by calling (866) 632-9992, or by writing a letter addressed to USDA. The letter must contain the complainant's name, address, telephone number, and a written description of the alleged discriminatory action in sufficient detail to inform the Assistant Secretary for Civil Rights (ASCR) about the nature and date of an alleged civil rights violation. The completed AD-3027 form or letter must be submitted to USDA by:

(a) *Mail:* U.S. Department of Agriculture, Office of the Assistant Secretary for Civil Rights, 1400 Independence Avenue SW, Washington, DC 20250-9410; or

(b) *Fax:* (833) 256-1665 or (202) 690-7442; or

(c) *Email:* program.intake@usda.gov.

USDA is an equal opportunity provider, employer, and lender.

Kathryn E. Dirksen Londrigan,

Administrator, Rural Business-Cooperative Service, USDA Rural Development.

[FR Doc. 2024-07136 Filed 4-3-24; 8:45 am]

BILLING CODE 3410-XY-P

COMMISSION ON CIVIL RIGHTS

Notice of Public Meeting of the Tennessee Advisory Committee

AGENCY: Commission on Civil Rights.

ACTION: Announcement of meeting.

SUMMARY: Notice is hereby given, pursuant to the provisions of the rules and regulations of the U.S. Commission on Civil Rights (Commission), and the Federal Advisory Committee Act (FACA) that a meeting of the Tennessee Advisory Committee to the Commission will convene by Zoom on Thursday, April 11, 2024, at 3:30 p.m. (CT). The purpose of the meeting is to discuss their draft report on Voting Rights.

DATES: The meeting will take place on Thursday, April 11, 2024, at 3:30 p.m. (CST).

Registration Link (Audio/Visual):
https://www.zoomgov.com/webinar/register/WN_5ETd-ID2Qli7oJJPqnA49A.

Telephone (Audio Only): Dial (833) 568-8864 USA Toll Free; Access Code: 161 235 6880.

FOR FURTHER INFORMATION CONTACT:

Victoria Moreno at vmoreno@usccr.gov or by phone at 434-515-0204.

SUPPLEMENTARY INFORMATION: This meeting is available to the public through the Zoom link above. If joining only via phone, callers can expect to incur charges for calls they initiate over wireless lines, and the Commission will not refund any incurred charges. Individuals who are deaf, deafblind and hard of hearing may also follow the proceedings by first calling the Federal Relay Service at 1-800-877-8339 and providing the Service with the call-in number found through registering at the web link provided above for the meeting.

Members of the public are entitled to make comments during the open period at the end of the meeting. Members of the public may also submit written comments; the comments must be received in the Regional Programs Unit within 30 days following the respective meeting. Written comments may be emailed to Victoria Moreno at vmoreno@usccr.gov. All written comments received will be available to the public.

Persons who desire additional information may contact the Regional Programs Unit at (202) 809-9618. Records and documents discussed during the meeting will be available for public viewing as they become available at the www.facadatabase.gov. Persons interested in the work of this advisory committee are advised to go to the Commission's website, www.usccr.gov, or to contact the Regional Programs Unit at the above phone number or email address.

Agenda

Thursday, April 11, 2024, at 3:30 p.m. (CST)

1. Welcome & Roll Call
2. Chair's Comments
3. Discussion on Report
4. Next Steps
5. Public Comment
6. Adjourn

Dated: April 1, 2024.

David Mussatt,

Supervisory Chief, Regional Programs Unit.

[FR Doc. 2024-07158 Filed 4-3-24; 8:45 am]

BILLING CODE P

DEPARTMENT OF COMMERCE

International Trade Administration

[A-580-904]

Forged Steel Fittings From the Republic of Korea: Final Results of Antidumping Duty Administrative Review; 2021-2022

AGENCY: Enforcement and Compliance, International Trade Administration, Department of Commerce.

SUMMARY: The U.S. Department of Commerce (Commerce) determines that Samyoung Fitting Co., Ltd. (Samyoung), a producer/exporter subject to this administrative review, made sales of forged steel fittings at less than normal value. The period of review (POR) is December 1, 2021, through November 31, 2022.

DATES: Applicable April 4, 2024.

FOR FURTHER INFORMATION CONTACT:

Daniel Alexander, AD/CVD Operations, Office VII, Enforcement and Compliance, International Trade Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Washington, DC 20230; telephone: (202) 482-4313.

SUPPLEMENTARY INFORMATION:

Background

On September 25, 2023, Commerce published the *Preliminary Results* for this review in the **Federal Register** and

invited interested parties to comment on those results.¹ From October 26 to November 1, 2023, interested parties submitted case and rebuttal briefs.² For a complete description of the events that occurred since Commerce published the *Preliminary Results*, see the Issues and Decision Memorandum.³ Commerce conducted this review in accordance with section 751(a) of the Tariff Act of 1930, as amended (the Act).

Scope of the Order⁴

The merchandise subject to the *Order* is forged steel fittings from the Republic of Korea. For a complete description of the scope of the *Order*, see the Issues and Decision Memorandum.

Analysis of Comments Received

All issues raised in the case and rebuttal briefs filed by parties in this review are listed in the appendix to this notice and addressed in the Issues and Decision Memorandum. The Issues and Decision Memorandum is a public document and is on file electronically via Enforcement and Compliance's Antidumping and Countervailing Duty Centralized Electronic Service System (ACCESS). ACCESS is available to registered users at <https://access.trade.gov>. In addition, a complete version of the Issues and Decision Memorandum can be accessed directly at <https://access.trade.gov/public/FRNoticesListLayout.aspx>.

Changes Since the Preliminary Results

Based on a review of the record and comments received from interested parties regarding the *Preliminary Results*, we made certain changes to the preliminary weighted-average dumping margin calculated for Samyoung. For a detailed discussion of these changes, see the Issues and Decision Memorandum.⁵

¹ See *Forged Steel Fittings from the Republic of Korea: Preliminary Results of Antidumping Duty Administrative Review*, 88 FR 65653 (September 25, 2023) (*Preliminary Results*), and accompanying Preliminary Decision Memorandum.

² See Samyoung's Letter, "Case Brief," dated October 25, 2023; see also Bonney Forge Corporation's Letter, "Bonney Forge Corporation's Case Brief," dated October 26, 2023; and Samyoung's Letter, "Rebuttal Brief," dated November 1, 2021.

³ See Memorandum, "Forged Steel Fittings from the Republic of Korea: Issues and Decision Memorandum for the Final Results of the Antidumping Duty Administrative Review; 2021–2022," dated concurrently with, and hereby adopted by, this notice (Issues and Decision Memorandum).

⁴ See *Forged Steel Fittings from the Republic of Korea: Final Affirmative Determination of Sales at Less Than Fair Value*, 85 FR 66302 (October 19, 2020) (*Order*).

⁵ See Issues and Decision Memorandum at 4.

Final Results of Review

Exporter/producer	Weighted-average dumping margin (percent)
Samyoung Fitting Co., Ltd	3.99

Disclosure

Commerce intends to disclose its calculations and analysis performed to interested parties in these final results within five days of the date of publication of this notice, in accordance with 19 CFR 351.224(b).

Assessment Rates

Pursuant to section 751(a)(2)(C) of the Act, and 19 CFR 351.212(b)(1), Commerce has determined, and U.S. Customs and Border Protection (CBP) shall assess, antidumping duties on all appropriate entries of subject merchandise in accordance with the final results of this review.

Pursuant to 19 CFR 351.212(b)(1), Samyoung reported the entered value of its U.S. sales such that we calculated importer-specific *ad valorem* duty assessment rates based on the ratio of the total amount of dumping calculated for the examined sales to the total entered value of the sales for which entered value was reported. Where either the respondent's weighted-average dumping margin is zero or *de minimis* within the meaning of 19 CFR 351.106(c)(1), or an importer-specific assessment rate is zero or *de minimis*, we will instruct CBP to liquidate the appropriate entries without regard to antidumping duties.

Commerce's "automatic assessment" practice will apply to entries of subject merchandise during the POR produced by Samyoung for which the company did not know that the merchandise it sold to the intermediary (e.g., a reseller, trading company, or exporter) was destined for the United States. In such instances, we will instruct CBP to liquidate unreviewed entries at the all-others rate of 17.08 percent⁶ if there is no rate for the intermediate company(ies) involved in the transaction.

Commerce intends to issue liquidation instructions to CBP no earlier than 35 days after the date of publication of the final results of this review in the **Federal Register**. If a timely summons is filed at the U.S. Court of International Trade, the assessment instructions will direct CBP not to liquidate relevant entries until the time for parties to file a request for a

statutory injunction has expired (*i.e.*, within 90 days of publication).

Cash Deposit Requirements

The following cash deposit requirements will be effective for all shipments of the subject merchandise entered, or withdrawn from warehouse, for consumption on or after the publication date of the final results of this administrative review, as provided by section 751(a)(2)(C) of the Act: (1) the cash deposit rate for the company listed above will be equal to the weighted-average dumping margin established in the final results of this review, except if the rate is less than 0.50 percent and, therefore, *de minimis* within the meaning of 19 CFR 351.106(c)(1), in which case the cash deposit rate will be zero; (2) for previously investigated or reviewed companies not listed above, the cash deposit rate will continue to be the company-specific cash deposit rate published for the most recently completed segment; (3) if the exporter is not a firm covered in this review, or the original less-than-fair-value (LTFV) investigation, but the producer is, then the cash deposit rate will be the cash deposit rate established for the most recently completed segment for the producer of the merchandise; and (4) the cash deposit rate for all other producers or exporters will continue to be 17.08 percent, the all-others rate established in the LTFV investigation.⁷ These cash deposit requirements, when imposed, shall remain in effect until further notice.

Notification to Importers

This notice serves as a final reminder to importers of their responsibility under 19 CFR 351.402(f)(2) to file a certificate regarding the reimbursement of antidumping duties prior to liquidation of the relevant entries during this review period. Failure to comply with this requirement could result in Commerce's presumption that reimbursement of antidumping duties occurred and the subsequent assessment of double antidumping duties.

Administrative Protective Order

This notice serves as the only reminder to parties subject to an administrative protective order (APO) of their responsibility concerning the disposition of proprietary information disclosed under APO in accordance with 19 CFR 351.305(a)(3), which continues to govern business proprietary information in this segment of the proceeding. Timely written notification of return/destruction of

⁶ See *Order*.

⁷ *Id.*

APO materials or conversion to judicial protective order is hereby requested. Failure to comply with the regulations and the terms of an APO is a sanctionable violation.

Notification to Interested Parties

We are issuing and publishing these final results in accordance with sections 751(a)(1) and 777(i)(1) of the Act, and 19 CFR 351.221(b)(5).

Dated: March 21, 2024.

Ryan Majerus,

Deputy Assistant Secretary for Policy and Negotiations, performing the non-exclusive functions and duties of the Assistant Secretary for Enforcement and Compliance.

Appendix

List of Topics Discussed in the Issues and Decision Memorandum

- I. Summary
- II. Background
- III. Scope of the Order
- IV. Changes Since the Preliminary Results
- V. Discussion of the Issues
 - Comment 1: Revision of the Sales Window for the Final Results
 - Comment 2: Whether to Make Certain Adjustments to Home Market Fields
 - Comment 3: Whether to Make Changes to Margin Calculation Fields Regarding Value, Importer Name, and Differential Pricing Parameters
 - Comment 4: Correcting Certain Currency Conversions
- VI. Recommendation

[FR Doc. 2024-07123 Filed 4-3-24; 8:45 am]

BILLING CODE 3510-DS-P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[RTID 0648-XD845]

Caribbean Fishery Management Council; Public Meeting

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of public hybrid meeting (in-person/virtual).

SUMMARY: The Caribbean Fishery Management Council (CFMC) will hold the 184th public hybrid meeting to address the items contained in the tentative agenda included in the **SUPPLEMENTARY INFORMATION.**

DATES: The 184th CFMC public hybrid meeting will be held on April 23, 2024, from 9 a.m. to 4:30 p.m. A closed session will be held from 4:45 p.m. to 5:30 p.m., to discuss personnel matters, and on April 24, 2024, from 9 a.m. to 4:30 p.m. AST.

ADDRESSES:

Meeting address: The meeting will be held at the Courtyard by Marriott Isla Verde Beach Resort, 7012 Boca de Cangrejos Avenue, Carolina, Puerto Rico 00979.

You may join the 184th CFMC public hybrid meeting via Zoom, from a computer, tablet or smartphone by entering the following address:

Join Zoom Meeting
[https://us02web.zoom.us/j/83060685915?](https://us02web.zoom.us/j/83060685915?pwd=VmVsc1orSUtKck8xYk1XOXNDY1ErZz09)
 pwd=VmVsc1orSUtKck
 8xYk1XOXNDY1ErZz09

Meeting ID: 830 6068 5915

Passcode: 995658

One tap mobile

+17879451488,,83060685915#,,,,,0#,,
 995658# Puerto Rico
 +17879667727,,83060685915#,,,,,0#,,
 995658# Puerto Rico

Dial by your location

+1 787 945 1488 Puerto Rico
 +1 787 966 7727 Puerto Rico
 +1 939 945 0244 Puerto Rico

Meeting ID: 830 6068 5915

Passcode: 995658

In case there are problems, and we cannot reconnect via Zoom, the meeting will continue using GoToMeeting.

You can join the meeting from your computer, tablet, or smartphone. <https://global.gotomeeting.com/join/971749317>. You can also dial in using your phone. United States: +1 (408) 650-3123 Access Code: 971-749-317.

FOR FURTHER INFORMATION CONTACT:

Miguel A. Rolón, Executive Director, Caribbean Fishery Management Council, 270 Muñoz Rivera Avenue, Suite 401, San Juan, Puerto Rico 00918-1903; telephone: (787) 398-3717.

SUPPLEMENTARY INFORMATION: The following items included in the tentative agenda will be discussed:

April 23, 2024

9 a.m.–9:30 p.m.

- Call to Order
- Roll Call
- Adoption of Agenda
- Consideration of 183rd Council Meeting Verbatim Transcription
- Executive Director's Report

9:30 a.m.–10:10 a.m.

- Scientific and Statistical Committee Report—Vance Vicente, Chair
- Ecosystem-Based Fisheries Management Technical Advisory Panel Report—Sennai Habtes, Chair

10:10 a.m.–10:50 a.m.

- Southeast Fishery Science Center Updates—Kevin McCarthy, Caribbean Fisheries Branch, NOAA Fisheries

- Harvest Control Rules in a Changing Environment: Lessons for Confronting Non-Stationarity in the U.S. Caribbean—Matt Damiano, Caribbean Fisheries Branch, SEFSC, NOAA Fisheries

10:50 a.m.–11 a.m.

—Coffee Break

11 a.m.–11:30 a.m.

- NMFS Southeast Equity and Environmental Justice (EEJ) Implementation Plan—NMFS SERO/SEFSC

11:30 a.m.–12:15 p.m.

- Fishery Management Plans (FMPs) Amendments and Actions Update—María López-Mercer, NOAA Fisheries

12:15 p.m.–1:15 p.m.

—Lunch Break

1:15 p.m.–2 p.m.

- Framework Action 3 under the Puerto Rico Fishery Management Plan: Modification of Status Determination Criteria and Management Reference Points for the Triggerfish Stock Complex based on the SEDAR 80 Queen Triggerfish Stock Assessment—Final Action, NMFS SERO Sustainable Fisheries

2 p.m.–3 p.m.

- Amendment 3 to the Puerto Rico, St. Croix, and St. Thomas and St. John Fishery Management Plans: Management Measures for Dolphin and Wahoo—Final Action, NMFS SERO Sustainable Fisheries

3 p.m.–3:15 p.m.

—Coffee Break

3:15 p.m.–4:15 p.m.

- Queen Conch Endangered Species Act Final Listing—NMFS SERO Protected Resources

4:15 p.m.–4:30 p.m.

- Public Comment Period (5-minute presentations)

4:30 p.m.

—Adjourn for the day

4:45 p.m.–5:30 p.m.

—Closed Session

April 24, 2024

9 a.m.–9:30 a.m.

- Building Successful Linkages in Support of the Queen Conch and Fish Spawning Aggregation Regional Fisheries Management Sustainability—Martha Prada

9:30 a.m.–10 a.m.

—Big Fish Campaign—Ana Salceda

10 a.m.–10:45 a.m.

—Outreach and Education Advisory Panel Report—Alida Ortíz

—CFMC Social Networks—Cristina Olan

10:45 a.m.–11 a.m.

—Coffee Break

11 a.m.–11:30 p.m.

—CFMC Liaison Officers Reports (10 minutes each)

—St. Croix, U.S.V.I.—Liandry De La Cruz

—St. Thomas/St. John, U.S.V.I.—Nicole Greaux

—Puerto Rico—Wilson Santiago

11:30 a.m.–11:45 p.m.

—Deed Water Snappers: Puerto Rico Regulations Update—Ricardo López, FRL, PR DNER

11:45 a.m.–12 p.m.

—Microplastics and Fisheries in Puerto Rico—Yesenia Marín/Ricardo López

12 p.m.–12:15 p.m.

—Shark Management Needs in Puerto Rico—Wanda Ortíz

12:15 p.m.–1:30 p.m.

—Lunch Break

1:30 p.m.–2:15 p.m.

—District Advisory Panel Reports (15 mins each)

—St. Thomas, U.S.V.I.—Julian Magras, Chair

—St. Croix, U.S.V.I.—Gerson Martinez, Chair

—Puerto Rico—Nelson Crespo, Chair

2:15 p.m.–2:30 p.m.

—Shipping Lanes in St. Croix, USVI—Carlos Farchette

2:30 p.m.–3:10 p.m.

—Enforcement Reports (10 minutes each)

—Puerto Rico DNER

—U.S.V.I. DPNR

—U.S. Coast Guard

—NOAA Fisheries Office of Law Enforcement

3:10 p.m.–3:30 p.m.

—Advisory Bodies Membership

3:30 p.m.–3:45 p.m.

—Other Business

3:45 p.m.–4:30 p.m.

—Public Comment Period (5-minute presentations)

—Next Meetings

4:30 p.m.

—Adjourn

Note (1): Other than starting time and dates of the meetings, the established times for addressing items on the agenda may be adjusted as necessary to accommodate the timely completion of discussion relevant to the agenda items. To further accommodate discussion and completion of all items on the agenda, the meeting may be extended from, or completed prior to the date established in this notice. Changes in the agenda will be posted to the CFMC website, Facebook, Twitter and Instagram as practicable.

Note (2): Financial disclosure forms are available for inspection at this meeting, as per 50 CFR part 601.

The order of business may be adjusted as necessary to accommodate the completion of agenda items. The meeting will begin on April 23, 2024, at 9 a.m. AST, and will end on April 24, 2024, at 4:30 p.m. AST. Other than the start time on the first day of the meeting, interested parties should be aware that discussions may start earlier or later than indicated in the agenda, at the discretion of the Chair.

Special Accommodations

For any additional information on this public virtual meeting, please contact Diana Martino, Caribbean Fishery Management Council, 270 Muñoz Rivera Avenue, Suite 401, San Juan, Puerto Rico 00918–1903; telephone: (787) 226–8849.

Authority: 16 U.S.C. 1801 *et seq.*

Dated: April 1, 2024.

Rey Israel Marquez,

Acting Deputy Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 2024–07186 Filed 4–3–24; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[RTID 0648–XD757]

Pacific Fishery Management Council; Public Meeting

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of public meeting.

SUMMARY: The Pacific Fishery Management Council's (Pacific Council) Ad-Hoc Klamath River Fall Chinook Workgroup will hold an online meeting.

DATES: The online meeting will be held Wednesday, April 24, 2024, from 9 a.m. until 3 p.m., Pacific daylight time, or until business for the day concludes.

ADDRESSES: This meeting will be held online. Specific meeting information, including directions on how to join the meeting and system requirements will be provided in the meeting announcement on the Pacific Council's website (see www.pcouncil.org). You may send an email to Mr. Kris Kleinschmidt (kris.kleinschmidt@noaa.gov) or contact him at (503) 820–2280, extension 412 for technical assistance.

Council address: Pacific Fishery Management Council, 7700 NE Ambassador Place, Suite 101, Portland, OR 97220–1384.

FOR FURTHER INFORMATION CONTACT: Robin Ehlke, Staff Officer, Pacific Council; telephone: (503) 820–2410.

SUPPLEMENTARY INFORMATION: The primary purpose of the meeting is to discuss and further develop interim management measures, or a management framework, intended to address the response of Klamath River fall Chinook to the dynamic nature of the Klamath River environment and the available habitat immediately following dam removal, and post dam removal until the natural environment is stabilized and the salmon population is more predictable. Additional discussions may include, but are not limited to, the work of the Sacramento River Fall Chinook Workgroup, future meetings, workload planning, and upcoming Council agenda items etc. may also occur. The Workgroup will provide their recommendations to the Council at their March 5–11 meeting in Fresno, CA.

Although non-emergency issues not contained in the meeting agenda may be discussed, those issues may not be the subject of formal action during this meeting. Action will be restricted to those issues specifically listed in this document and any issues arising after publication of this document that require emergency action under section 305(c) of the Magnuson-Stevens Fishery Conservation and Management Act, provided the public has been notified of the intent to take final action to address the emergency.

Special Accommodations

Requests for sign language interpretation or other auxiliary aids should be directed to Mr. Kris Kleinschmidt (kris.kleinschmidt@noaa.gov; (503) 820–2412) at least 10 days prior to the meeting date.

Authority: 16 U.S.C. 1801 *et seq.*

Dated: April 1, 2024.

Rey Israel Marquez,

Acting Deputy Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 2024-07184 Filed 4-3-24; 8:45 am]

BILLING CODE 3510-22-P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[RTID 0648-XD852]

North Pacific Fishery Management Council; Public Meeting

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of web conferences.

SUMMARY: The North Pacific Fishery Management Council (Council) is holding three pre-workshop discussion meetings in preparation for the Climate Scenario Workshop.

DATES: The meetings will be held on Wednesday, April 24, 2024, Tuesday, April 30, 2024, and on Tuesday, May 14, 2024, from 1 p.m. to 2 p.m., Alaska Time.

ADDRESSES: The meetings will be web conferences. Join online through the link at <https://meetings.npfmc.org/Meeting/Details/3042>.

Council address: North Pacific Fishery Management Council, 1007 W 3rd Ave., Suite 400, Anchorage, AK 99501-2252; telephone: (907) 271-2809. Instructions for attending the meeting are given under **SUPPLEMENTARY INFORMATION**, below.

FOR FURTHER INFORMATION CONTACT: Katie Latanich, Council staff; phone: (907) 271-2809 and email: katie.latanich@noaa.gov. For technical support, please contact our administrative staff; email: npfmc.admin@noaa.gov.

SUPPLEMENTARY INFORMATION:

Agenda

Wednesday, April 24, 2024

This session will review the anticipated climate change impacts to the Bering Sea, Aleutian Islands, and Gulf of Alaska, followed by a discussion of the challenges involved in planning for climate change effects that are likely to become more frequent and impactful. The agenda is subject to change, and the latest version will be posted at <https://meetings.npfmc.org/Meeting/Details/3042> prior to the meeting, along with meeting materials.

Tuesday, April 30, 2024

This session will explore the meaning of “climate readiness” through recent work including the Council’s Climate Readiness Synthesis Report, and community climate adaptation planning efforts, followed by a discussion of different perspectives on climate readiness. The agenda is subject to change, and the latest version will be posted at <https://meetings.npfmc.org/Meeting/Details/3042> prior to the meeting, along with meeting materials.

Tuesday, May 14, 2024

This session will provide an introduction to climate scenario planning and the scenarios that will be discussed at the NPFMC Climate Scenarios Workshop. This information will also be provided as briefing material and discussed at the workshop. The agenda is subject to change, and the latest version will be posted at <https://meetings.npfmc.org/Meeting/Details/3042> prior to the meeting, along with meeting materials.

Connection Information

You can attend the meeting online using a computer, tablet, or smart phone; or by phone only. Connection information will be posted online at: <https://meetings.npfmc.org/Meeting/Details/3042>.

Public Comment

Public comment letters will be accepted and should be submitted electronically to <https://meetings.npfmc.org/Meeting/Details/3042>.

Authority: 16 U.S.C. 1801 *et seq.*

Dated: April 1, 2024.

Rey Israel Marquez,

Acting Deputy Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 2024-07187 Filed 4-3-24; 8:45 am]

BILLING CODE 3510-22-P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[RTID 0648-XD815]

South Atlantic Fishery Management Council; Public Meetings

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of public meetings.

SUMMARY: The South Atlantic Fishery Management Council (Council) will hold a meeting of the Habitat and

Ecosystem Advisory Panel on April 22–24, 2024, and a joint meeting of the Shrimp and Deepwater Shrimp Advisory Panels on April 24–25, 2024.

DATES: The Habitat and Ecosystem Advisory Panel (AP) meeting will be held April 22, 2024, from 1 p.m. until 5 p.m.; April 23, 2024, from 9 a.m. until 5 p.m.; and April 24, 2024, from 9 a.m. until 1 p.m., EDT. The Joint Shrimp AP meeting will be held April 24, 2024, from 2 p.m. until 5 p.m. and April 25, 2024, from 8:30 a.m. until 5 p.m., EDT.

ADDRESSES:

Meeting address: The meetings will be held at the Crown Plaza, 4831 Tanger Outlet Blvd., North Charleston, SC 29418; toll free: (866) SAFMC-10; fax: (843) 769-4520.

Council address: South Atlantic Fishery Management Council, 4055 Faber Place Drive, Suite 201, N Charleston, SC 29405.

The meetings will also be available via webinar. Registration is required. Webinar registration, an online public comment form, and briefing book materials will be available two weeks prior to the meeting at: <https://safmc.net/advisory-panel-meetings/>.

FOR FURTHER INFORMATION CONTACT:

Kathleen Howington, Habitat and Ecosystem Scientist, Kathleen.howington@safmc.net; phone: (843) 725-7580 and Allie Iberle, Fishery Scientist, email: allie.iberle@safmc.net; phone: (843) 225-8135.

SUPPLEMENTARY INFORMATION:

Habitat and Ecosystem Advisory Panel

The Habitat and Ecosystem AP will review progress on the Essential Fish Habitat (EFH) 5-Year Review, review progress on integrating wind energy into the Council’s Energy Policy, prepare an annual habitat activities report, review website progress, and receive an update on the Council’s Citizen Science program. The AP will also discuss wind farm removal, Indian River Lagoon concerns, and the potential implications of Sackett vs Environmental Protection Agency. The AP will provide recommendations to the Council on other topics as needed.

Joint Shrimp and Deepwater Shrimp Advisory Panels

The Shrimp and Deepwater Shrimp APs will receive an update on the Council’s Citizen Science program and an update on Coral Amendment 10 addressing the shrimp fishery access area along the eastern boundary of the Oculina Bank Habitat Area of Particular Concern. AP members will provide a fishery performance report for shrimp and discuss economic issues within the

South Atlantic shrimp industry. The APs will review the Giant Manta Ray Biological Opinion from NOAA Fisheries and receive presentations from the Southern Shrimp Collaborative and the Shrimp Futures Project. The APs will provide input to the Council on other topics as needed.

Special Accommodations

These meetings are physically accessible to people with disabilities. Requests for auxiliary aid should be directed to the Council office (see **ADDRESSES**) 5 days prior to the meeting.

Note: The times and sequence specified in this agenda are subject to change.

Authority: 16 U.S.C. 1801 *et seq.*

Dated: April 1, 2024.

Rey Israel Marquez,

Acting Deputy Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 2024-07185 Filed 4-3-24; 8:45 am]

BILLING CODE 3510-22-P

DEPARTMENT OF EDUCATION

[Docket No.: ED-2024-SCC-0054]

Agency Information Collection Activities; Comment Request; Reaffirmation Agreement

AGENCY: Federal Student Aid (FSA), Department of Education (ED).

ACTION: Notice.

SUMMARY: In accordance with the Paperwork Reduction Act (PRA) of 1995, the Department is proposing an extension without change of a currently approved information collection request (ICR).

DATES: Interested persons are invited to submit comments on or before June 3, 2024.

ADDRESSES: To access and review all the documents related to the information collection listed in this notice, please use <http://www.regulations.gov> by searching the Docket ID number ED-2024-SCC-0054. Comments submitted in response to this notice should be submitted electronically through the Federal eRulemaking Portal at <http://www.regulations.gov> by selecting the Docket ID number or via postal mail, commercial delivery, or hand delivery. If the [regulations.gov](http://www.regulations.gov) site is not available to the public for any reason, the Department will temporarily accept comments at ICDocketMgr@ed.gov. Please include the docket ID number and the title of the information collection request when requesting documents or submitting comments. Please note that comments submitted

after the comment period will not be accepted. Written requests for information or comments submitted by postal mail or delivery should be addressed to the Manager of the Strategic Collections and Clearance Governance and Strategy Division, U.S. Department of Education, 400 Maryland Ave. SW, LBJ, Room 6W203, Washington, DC 20202-8240.

FOR FURTHER INFORMATION CONTACT: For specific questions related to collection activities, please contact Beth Grebeldinger, 202-377-4018.

SUPPLEMENTARY INFORMATION: The Department, in accordance with the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3506(c)(2)(A)), provides the general public and Federal agencies with an opportunity to comment on proposed, revised, and continuing collections of information. This helps the Department assess the impact of its information collection requirements and minimize the public's reporting burden. It also helps the public understand the Department's information collection requirements and provide the requested data in the desired format. The Department is soliciting comments on the proposed information collection request (ICR) that is described below. The Department is especially interested in public comment addressing the following issues: (1) is this collection necessary to the proper functions of the Department; (2) will this information be processed and used in a timely manner; (3) is the estimate of burden accurate; (4) how might the Department enhance the quality, utility, and clarity of the information to be collected; and (5) how might the Department minimize the burden of this collection on the respondents, including through the use of information technology. Please note that written comments received in response to this notice will be considered public records.

Title of Collection: Reaffirmation Agreement.

OMB Control Number: 1845-0133.

Type of Review: An extension without change of a currently approved ICR.

Respondents/Affected Public: Individuals and Households; Private Sector; State, Local, and Tribal Governments.

Total Estimated Number of Annual Responses: 8,594.

Total Estimated Number of Annual Burden Hours: 1,032.

Abstract: The Higher Education Act of 1965, as amended (HEA), established the Federal Family Education Loan (FFEL) Program, and the William D. Ford Federal Direct Loan (Direct Loan) Program under Title IV, Parts B and D

respectively. The HEA provides for a maximum loan amount that a borrower can receive per year and in total. If a borrower receives more than the maximum amount, the borrower becomes ineligible for further Title IV aid (including Federal Pell Grants, Federal Supplemental Educational Opportunity Grants, Federal Work-Study, and Teacher Education Assistance for Higher Education (TEACH) Grants, Iraq and Afghanistan Service Grants) unless the borrower repays the excess amount or agrees to repay the excess amount according to the terms and conditions of the promissory note that the borrower signed. Agreeing to repay the excess amount according to the terms and conditions of the promissory note that the borrower signed is called reaffirmation, which is the subject of this collection. This renewal without change of the information collection is necessary for the Department of Education (the Department), as a holder of some FFEL Program loans and all Direct Loans, and all FFEL Program lenders to capture the borrowers formal agreement to repay any excess amount of FFEL or Direct Loan program loans that the borrower received according to the terms and conditions of the promissory note the borrower signed. The form has not been changed since its last update.

Dated: April 1, 2024.

Kun Mullan,

PRA Coordinator, Strategic Collections and Clearance, Governance and Strategy Division, Office of Chief Data Officer, Office of Planning, Evaluation and Policy Development.

[FR Doc. 2024-07151 Filed 4-3-24; 8:45 am]

BILLING CODE 4000-01-P

DEPARTMENT OF EDUCATION

Applications for New Awards; Augustus F. Hawkins Centers of Excellence Program

AGENCY: Office of Postsecondary Education, Department of Education.

ACTION: Notice.

SUMMARY: The Department of Education (Department) is issuing a notice inviting applications for fiscal year (FY) 2024 for the Augustus F. Hawkins Centers of Excellence (Hawkins) Program, Assistance Listing Number (ALN) 84.428A. This notice relates to the approved information collection under OMB control number 1894-0006.

DATES:

Applications Available: April 4, 2024.

Deadline for Transmittal of Applications: June 18, 2024.

Deadline for Intergovernmental Review: August 19, 2024.

ADDRESSES: For the addresses for obtaining and submitting an application, please refer to our Common Instructions for Applicants to Department of Education Discretionary Grant Programs, published in the **Federal Register** on December 7, 2022 (87 FR 75045), and available at <https://www.federalregister.gov/documents/2022/12/07/2022-26554/common-instructions-for-applicants-to-department-of-education-discretionary-grant-programs>.

FOR FURTHER INFORMATION CONTACT: Dr. Vicki Robinson, U.S. Department of Education, 400 Maryland Avenue SW, 5th Floor, Washington, DC 20202. Telephone: (202) 453-7907. Email: Vicki.Robinson@ed.gov. You may also contact Ashley Hillary, U.S. Department of Education, 400 Maryland Avenue SW, 5th Floor, Washington, DC 20202. Telephone: (202) 453-7880. Email: Ashley.Hillary@ed.gov.

If you are deaf, hard of hearing, or have a speech disability and wish to access telecommunications relay services, please dial 7-1-1.

SUPPLEMENTARY INFORMATION:

Full Text of Announcement

I. Funding Opportunity Description

Purpose of Program: The Hawkins Program, authorized under part B of title II of the Higher Education Act of 1965, as amended (HEA), is designed to support comprehensive, high-quality State-accredited teacher preparation programs by creating centers of excellence at Historically Black Colleges and Universities (HBCUs); Tribal Colleges or Universities (TCUs); or Minority Serving Institutions (MSIs), such as Hispanic-Serving Institutions (HSIs). The Hawkins Program will help increase the number of, and retain, well-prepared teachers from diverse backgrounds, resulting in a more diverse teacher workforce prepared to teach in our Nation's most underserved elementary and secondary schools and close student opportunity and achievement gaps. This program focuses on the various aspects of the teacher preparation pipeline, including the recruitment, preparation, support, placement, retention, and retraining of teachers for and in under-resourced schools to support underserved students. Through this program, the Secretary seeks to fund applicants that propose to incorporate evidence-based practices into their teacher preparation program.

Background:

The Hawkins Program is critical in enabling the Department to meet its goal of supporting a diverse teacher workforce to improve student opportunities, achievement, and outcomes, and address the educator shortage, by providing expanded access to comprehensible, high-quality, and affordable educator preparation programs.

There is significant inequity in students' access to well-prepared, experienced, and effective teachers,¹ particularly for students from low-income backgrounds, students of color, children or students with disabilities, and English learners (ELs).² Providing all students with consistent access to well-prepared, effective, and diverse educators who provide high-quality instruction and support is essential to closing opportunity and achievement gaps. Teachers who entered the profession through the least comprehensive teacher preparation pathway are two to three times more likely to leave their school or the profession compared to those who entered through a comprehensive pathway.³ Research demonstrates that high rates of turnover harm student achievement,⁴ and that the quality of a school's leadership is among the most important predictors of teacher turnover, with more effective principals being more likely to retain their best teachers.⁵

Extensive, high-quality, and evidence-based clinical experience is one of three "aspects of preparation that have the highest potential for effects on outcomes for students."⁶ There are several ways

¹ Isenberg, E., Max, J., Gleason, P., Johnson, M., Deutsch, J., and Hansen, M. (2016). Do Low-Income Students Have Equal Access to Effective Teachers? Evidence from 26 Districts (NCEE 2017-4007). Washington, DC: National Center for Education Evaluation and Regional Assistance, Institute of Education Sciences, U.S. Department of Education.

² www.ed.gov/raisethebar/eliminating-educator-shortages-through-increasing-educator-diversity.

³ Ingersoll, R., & May, H. (2011). Recruitment, retention and the minority teacher shortage. CPRE Research Report #R-69. Philadelphia, PA: Consortium for Policy Research in Education, University of Pennsylvania.

⁴ Carver-Thomas, D., and Darling-Hammond, L. (2017). Teacher Turnover: Why It Matters and What We Can Do About It, Learning Policy Institute, <https://learningpolicyinstitute.org/product/teacher-turnover-report>.

⁵ Grissom, J. (2018). Strong principals retain effective teachers—and don't retain ineffective ones, The Brookings Institution, <https://www.brookings.edu/articles/strong-principals-retain-effective-teachers-and-dont-retain-ineffective-ones/>.

⁶ National Research Council. (2010). Preparing teachers: Building evidence for sound policy. Report by the Committee on the study of teacher preparation programs in the United States. Washington, DC: National Academies Press.

educator preparation programs can partner with school districts and schools to provide these kinds of clinical experiences. For example, a number of school districts are partnering with teacher preparation programs to provide clinical experiences that are mutually beneficial for teacher candidates and teachers of record, and their students. Teacher candidates, in addition to completing the required elements of an evidence-based clinical experience, may serve in schools in roles that support students and teachers as their academic schedules allow and as they complete their other requirements for teacher certification. Teacher residencies and Grow Your Own⁷ programs, which may be supported through registered teacher apprenticeship programs, can support teacher candidates serving in these roles and cover the costs associated with extensive clinical experience. Other examples of educator preparation programs supporting high need schools in this way can be found here: www.ed.gov/coronavirus/factsheets/teacher-shortage.

While the majority of U.S public school students are children of color,⁸ only 20 percent of teachers are people of color. Further, 40 percent of the Nation's public schools do not employ a single teacher of color on record.⁹ Research shows that teachers of color benefit all students and can have a significant positive impact on students of color.¹⁰ These benefits can include higher levels of achievement,¹¹ greater encouragement, increased students' aspirations (e.g., through role modeling), more recommendations from teachers (e.g., to gifted and talented programs), and increased access to rigorous course-taking.¹² Research also demonstrates

⁷ Motamedi, J., Leong, M., and Yoon, S. (2017). Strategies for Designing, Implementing, and Evaluating Grow-Your-Own Teacher Programs for Educators, REL Northwest, <https://ies.ed.gov/ncee/edlabs/regions/northwest/pdf/strategies-for-educators.pdf>.

⁸ <https://nces.ed.gov/programs/coe/indicator/cge/racial-ethnic-enrollment>.

⁹ Education Trust (2022). Educators of Color Make the Case for Teacher Diversity. <https://edtrust.org/wp-content/uploads/2014/09/Educators-of-Color-Make-the-Case-for-Teacher-Diversity-November-2022.pdf>.

¹⁰ Dee, T. (2004). Teachers, race and student achievement in a randomized experiment. The Review of Economics and Statistics, 86(1), 195-210; and Gershenson, S., Hart, C.M.D., Lindsay, C.A., & Papageorge, N.W. (2017). The long-run impacts of same race teachers. Bonn, Germany: IZA Institute of Labor Economics. Discussion Paper Series.

¹¹ Egalite, A., Kisida, B., & Winters, M.A. Representation in the classroom: The effect of own-race teachers on student achievement, Economics of Education Review, 45 (April 2015), 44-52.

¹² Grissom, J., Kabourek, S., & Kramer, J. Exposure to same-race or same-ethnicity teachers and

that teachers of color can be positive role models for all students in breaking down negative stereotypes and preparing students to live and work in a multiracial society.¹³ A more diverse teacher workforce also increases the likelihood that students of color will have access to culturally and linguistically relevant teaching and learning and positive relationships.¹⁴ Thus, supporting teachers of color can be a critical strategy for advancing educational equity for students of color and addressing one of the root causes of institutional barriers to equity in the academic environment.¹⁵

In addition to the need for more teachers of color, a parallel challenge in the Nation's public schools lies in the shortage of multilingual teachers prepared to teach a growing population of English Learners (ELs). ELs are the fastest growing student demographic, with more than 10 percent of students identified as ELs currently.¹⁶ Additionally, about one-quarter of all students speak a language other than English at home, whereas only 1 in 8 teachers do.¹⁷ Despite that, more than half of the States nationwide are experiencing bilingual and multilingual teacher shortages and a quarter of the States do not require certification or endorsements for teachers who teach ELs.¹⁸

Research demonstrates that ELs who are taught in bilingual settings, such as dual-language immersion programs, by well-prepared bilingual teachers have stronger academic outcomes and better English-language acquisition trajectories than ELs who are taught in English only settings, which underscores the need to close the multilingual teacher shortage gap.¹⁹ Additionally, ELs who learn in

advanced math course-taking in high school: Evidence from a diverse urban district, *Teachers College Record*, 122 (2020), 1–42.

¹³ www2.ed.gov/rschstat/eval/highered/racial-diversity/state-racial-diversity-workforce.pdf.

¹⁴ Blazar, D. (2021). *Teachers of Color, Culturally Responsive Teaching, and Student Outcomes: Experimental Evidence from the Random Assignment of Teachers to Classes*. (EdWorkingPaper: 21–501). Retrieved from Annenberg Institute at Brown University: <https://doi.org/10.26300/jym0-wz02>.

¹⁵ www2.ed.gov/rschstat/eval/highered/racial-diversity/state-racial-diversity-workforce.pdf.

¹⁶ https://nces.ed.gov/programs/digest/d20/tables/dt20_204.20.asp.

¹⁷ <https://datacenter.kidscount.org/data/tables/81-children-who-speak-a-language-other-than-english-at-home?loc=1&loc=1#detailed/1/any/false/1729,37,871,870,573,869,36,868,867,133/any/396,397>.

¹⁸ Torre Gibney, D., Kelly, H., Rutherford-Quach, S., Ballen Riccards, J., & Parker, C. (2021). *Addressing the bilingual teacher shortage*. CCNetwork.

¹⁹ Steele, J., Slater, R., Zamarró, G., Miller, T., Li, J., Burkhauser, S., Bacon, M. (2017). *Effects of Dual-*

bilingual settings in which they can maintain their native languages while learning English have stronger social and emotional development, cross-cultural skills, and problem-solving skills.²⁰ Bilingual and multilingual learning environments can also mitigate linguistic barriers that limit family engagement, as bilingual and multilingual teachers are more likely to communicate with linguistically diverse families and ensure they have equitable access to information about their students' education.²¹ Bilingual and multilingual teachers' assets are critical to creating inclusive school and family partnerships where linguistically diverse families can meaningfully participate in their child's education.²²

Through the priorities in this competition, the Department seeks to encourage HBCUs, TCUs, and MSIs to propose projects that are designed to increase and retain the number of well-prepared teachers from diverse backgrounds; increase evidence-based, comprehensive pre-service clinical experiences through teacher preparation programs; and increase the number of bilingual and/or multilingual teachers with full certification.

Priorities: This notice contains two absolute priorities and two competitive preference priorities. The absolute priorities and Competitive Preference Priority 1 are from the Notice of Final Priorities, Requirements, and Definitions for this program published elsewhere in this issue of the **Federal Register** (2024 NFP), and Competitive Preference Priority 2 is from the Secretary's Final Administrative Priorities for Discretionary Grant Programs published in the **Federal Register** on March 9, 2020 (85 FR 13640) (Administrative Priorities).

Absolute Priorities: For the FY 2024 grant competition and any subsequent year in which we make awards from the list of unfunded applications from this

Language Immersion Programs on Student Achievement: Evidence From Lottery Data, *American Educational Research Journal*, 54, no. 1S., 282S–306S, <https://journals.sagepub.com/doi/abs/10.3102/0002831216634463>.

²⁰ Williams, C., Soto-Boykin, X., Zabala, J., & Meek, S. (2023). *Why We Need to Cultivate America's Multilingual, Multicultural Assets*. The Century Foundation. <https://tcf.org/content/report/why-we-need-to-cultivate-americas-multilingual-multicultural-assets/#easy-footnote-bottom-9>.

²¹ Hopkins, M., & Schutz, K.M. (2019). *Bilingual teacher leadership: Supporting linguistically responsive practices and parent engagement in schools*. *NABE Journal of Research and Practice*, 9(2), 96–109.

²² Newcomer, S.N., & Puzio, K. (2016). "Cultivando confianza": A bilingual community of practice negotiates restrictive language policies. *International Journal of Bilingual Education and Bilingualism*, 19(4), 347–369.

competition, these priorities are absolute priorities. Under 34 CFR 75.105(c)(3), we consider only applications that meet both priorities.

These priorities are:

Absolute Priority 1: Projects that are Designed to Increase and Retain the Number of Well-Prepared Teachers from Diverse Backgrounds.

To meet this priority, an eligible applicant must propose projects that are designed to increase the number of well-prepared teachers and the diversity of the teacher workforce with a focus on increasing and retaining a diverse teacher workforce, and improving the preparation, recruitment, retention, and placement of such teachers.

Applicants addressing this priority must describe—

(a) How their project will integrate multiple services or initiatives across academic and student affairs, such as academic advising, counseling, stipends, child-care, structured/guided pathways from teacher candidates' first year in the preparation program through successful employment placement, career services, or student financial aid, such as scholarships, with the goal of increasing program completion and credential attainment;

(b) Their plan for identifying and supporting teacher candidates from backgrounds that are underrepresented in the profession, including teacher candidates of color. This plan must span the beginning of the preparation program through graduation, and include a plan to improve program entry rates, as applicable, graduation rates, passage rates for certification and licensure exams, and rates of successful employment placement between teacher candidate subgroups and an institution's overall teacher candidate population; and

(c) Their proposed initiatives to promote the retention of teachers from backgrounds that are underrepresented in the profession, including teachers of color, prepared through the program, which may include induction programs, such as teacher or school leader induction programs, or mentorship programs that provide school and district leaders with the support they need to persist in their professions.

Absolute Priority 2: Increase Evidence-Based, Comprehensive Pre-service Clinical Experiences Through Teacher Preparation Programs.

To meet this priority, an eligible applicant must propose projects that are evidence-based (as defined in 34 CFR 77.1) comprehensive teacher preparation programs that provide extensive clinical experience. Applicants with existing programs must

describe their record in graduating highly skilled, well-prepared, and diverse teachers and describe how the proposed project will refine or enhance existing programs. Applicants proposing new programs must describe how their new program is evidence-based and designed to achieve the intended outcomes of the Hawkins Program. Applicants must also address how they will—

(a) Examine the sources of inequity and inadequacy in resources and opportunity and implement pedagogical practices in teacher preparation programs that are inclusive with regard to race, ethnicity, culture, language, gender, and disability status and that prepare teachers to create inclusive, supportive, equitable, unbiased, and identity-safe learning environments for their students;

(b) Prepare teacher candidates to integrate rigorous academic content, including through the effective use of technology, and instructional techniques and strategies consistent with universal design for learning principles;

(c) Prepare teacher candidates to design and deliver instruction in ways that are engaging and provide their students with opportunities to think critically and solve complex problems, apply learning in authentic and real-world settings, communicate and collaborate effectively, and develop growth mindsets. Teacher candidate pedagogy should include how to incorporate project-based, work-based, or other experiential learning opportunities in curriculum development;

(d) Prepare teacher candidates to build meaningful and trusting relationships with students and their families to support in-home, community-based, and in-school learning; and

(e) Provide sustained and high-quality pre-service clinical experiences, including teaching assistant initiatives, that facilitate the pathway to the teaching credential for those with paraprofessional experience or high-quality school leader pre-service training, induction, and support in the first three years of school leadership for principals and other school leaders. In designing such experiences, applicants must consider opportunities to provide pre-service clinical experience earlier in the teacher preparation program, as is practicable, and in ways that benefit students and teachers. These clinical experiences must be designed to—

(1) Integrate pedagogy and classroom practice and promote effective teaching skills in academic content areas;

(2) Be tightly aligned with course work with clear, relevant, and strong links between theory and practice;

(3) Group teacher candidates in cohorts to facilitate reflection of practice and professional collaboration;

(4) Closely supervise interaction between teacher candidates and faculty, experienced teachers, principals, and other administrators in high-need schools or hard-to-staff schools; and

(5) Provide high-quality-teacher mentoring.

Competitive Preference Priorities: For the FY 2024 grant competition and any subsequent year in which we make awards from the list of unfunded applications from this competition, these priorities are competitive preference priorities. Under 34 CFR 75.105 (c)(2)(i), we award up to an additional 5 points to an application, depending on how well the application meets Competitive Preference Priority 1; and we award an additional 5 points to an application that meets Competitive Preference Priority 2.

These priorities are:

Competitive Preference Priority 1: Increasing the Number of Bilingual and/or Multilingual Teachers with Full Certification. (up to 5 points)

To meet this priority, an eligible applicant must propose projects that are designed to prepare effective and experienced bilingual and/or multilingual teachers for high-need schools by increasing the number of teachers across elementary and secondary schools who are fully certified to provide academic language instruction in a language other than English, including for English Learners (ELs). These projects must prepare teacher candidates to lead students toward linguistic fluency and academic achievement in more than one language. Applicants must describe—

(a) How their project will integrate multiple services or initiatives across academic and student affairs, such as academic advising, counseling, stipends, child-care, structured/guided pathways from teacher candidates' first year in the preparation program through successful employment placement, career services, or student financial aid, such as scholarships, and provide the necessary knowledge and skills so that teacher candidates can serve students from many different language backgrounds; and

(b) Their plan for recruiting, supporting, and retaining bilingual and/or multilingual teacher candidates, including those who may have a teaching credential but have not been teaching in bilingual and/or multilingual education settings; aspiring

teachers; and teaching assistants who are interested in becoming bilingual and/or multilingual teachers.

Competitive Preference Priority 2: Applications From New Potential Grantees (5 points)

(a) To meet this priority, an applicant must demonstrate that it does not, as of the deadline date for submission of applications, have an active grant, including through membership in a group application submitted in accordance with 34 CFR 75.127–75.129, under the Hawkins Program.

(b) For the purpose of this priority, a grant or contract is active until the end of the grant's or contract's project or funding period, including any extensions of those periods that extend the grantee's or contractor's authority to obligate funds.

Definitions: The definitions below apply to this competition and are from 34 CFR part 77.1, 20 U.S.C. 1033, and the 2024 NFP.

Demonstrates a rationale means a key project component included in the project's logic model is informed by research or evaluation findings that suggest the project component is likely to improve relevant outcomes.

Experimental study means a study that is designed to compare outcomes between two groups of individuals (such as students) that are otherwise equivalent except for their assignment to either a treatment group receiving a project component or a control group that does not. Randomized controlled trials, regression discontinuity design studies, and single-case design studies are the specific types of experimental studies that, depending on their design and implementation (e.g., sample attrition in randomized controlled trials and regression discontinuity design studies), can meet What Works Clearinghouse (WWC) standards without reservations as described in the WWC Handbooks:

(1) A randomized controlled trial employs random assignment of, for example, students, teachers, classrooms, or schools to receive the project component being evaluated (the treatment group) or not to receive the project component (the control group).

(2) A regression discontinuity design study assigns the project component being evaluated using a measured variable (e.g., assigning students reading below a cutoff score to tutoring or developmental education classes) and controls for that variable in the analysis of outcomes.

(3) A single-case design study uses observations of a single case (e.g., a student eligible for a behavioral intervention) over time in the absence

and presence of a controlled treatment manipulation to determine whether the outcome is systematically related to the treatment.

Logic model (also referred to as a theory of action) means a framework that identifies key project components of the proposed project (*i.e.*, the active “ingredients” that are hypothesized to be critical to achieving the relevant outcomes) and describes the theoretical and operational relationships among the key project components and relevant outcomes.

Note: In developing logic models, applicants may want to use resources such as the Regional Educational Laboratory Program’s (REL Pacific) Education Logic Model Application, available at <https://ies.ed.gov/ncee/edlabs/regions/pacific/elm.asp>. Other sources include: https://ies.ed.gov/ncee/edlabs/regions/pacific/pdf/REL_2014025.pdf, https://ies.ed.gov/ncee/edlabs/regions/pacific/pdf/REL_2014007.pdf, and https://ies.ed.gov/ncee/edlabs/regions/northeast/pdf/REL_2015057.pdf.

Pre-service means the period of training for a person who does not have a prior teaching certification or license and who is enrolled in a State-approved teacher education program at an institution of higher education, prior to becoming the teacher of record.

Project component means an activity, strategy, intervention, process, product, practice, or policy included in a project. Evidence may pertain to an individual project component or to a combination of project components (*e.g.*, training teachers on instructional practices for English learners and follow-on coaching for these teachers).

Promising evidence means that there is evidence of the effectiveness of a key project component in improving a relevant outcome, based on a relevant finding from one of the following:

(1) A practice guide prepared by WWC reporting a “strong evidence base” or “moderate evidence base” for the corresponding practice guide recommendation;

(2) An intervention report prepared by the WWC reporting a “positive effect” or “potentially positive effect” on a relevant outcome with no reporting of a “negative effect” or “potentially negative effect” on a relevant outcome; or

(3) A single study assessed by the Department, as appropriate, that—

(i) Is an experimental study, a quasi-experimental design study, or a well-designed and well-implemented correlational study with statistical controls for selection bias (*e.g.*, a study using regression methods to account for

differences between a treatment group and a comparison group); and

(ii) Includes at least one statistically significant and positive (*i.e.*, favorable) effect on a relevant outcome.

Quasi-experimental design study means a study using a design that attempts to approximate an experimental study by identifying a comparison group that is similar to the treatment group in important respects. This type of study, depending on design and implementation (*e.g.*, establishment of baseline equivalence of the groups being compared), can meet WWC standards with reservations, but cannot meet WWC standards without reservations, as described in the WWC Handbooks.

Relevant outcome means the student outcome(s) or other outcome(s) the key project component is designed to improve, consistent with the specific goals of the program.

Scientifically based reading research—

(1) Means research that applies rigorous, systemic, and objective procedures to obtain valid knowledge relevant to reading development, reading instruction, and reading difficulties; and

(2) Includes research that—

(i) Employs systemic, empirical methods that draw on observation or experiment;

(ii) Involves rigorous data analyses that are adequate to test the stated hypotheses and justify the general conclusions drawn;

(iii) Relies on measurements or observational methods that provide valid data across evaluators and observers and across multiple measurements and observations; and

(iv) Has been accepted by a peer-reviewed journal or approved by a panel of independent experts through a comparably rigorous, objective, and scientific review.

What Works Clearinghouse (WWC) Handbooks (WWC Handbooks) means the standards and procedures set forth in The WWC Standards Handbook, Versions 4.0 or 4.1, and WWC Procedures Handbook, Versions 4.0 or 4.1, or in the WWC Procedures and Standards Handbook, Version 3.0 or Version 2.1 (all incorporated by reference, see § 77.2). Study findings eligible for review under WWC standards can meet WWC standards without reservations, meet WWC standards with Reservations, or not meet WWC standards. WWC practice guides and intervention reports include findings from systematic reviews of evidence as described in the WWC Handbooks documentation.

Note: The WWC Procedures and Standards Handbook (Version 4.1), as well as the more recent WWC Handbook released in August 2022 (Version 5.0), are available at <https://ies.ed.gov/ncee/wwc/Handbooks>.

Application Requirements: The following application requirements for FY 2024 are from section 242(b) of the HEA (20 U.S.C. 1033a(b)).

Grants provided by the Secretary must be used to ensure that current and future teachers meet the applicable State certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special education teachers, the qualifications described in section 612(a)(14)(C) of the Individuals with Disabilities Education Act (IDEA), by carrying out one or more of the following activities:

(1) Implementing reforms within teacher preparation programs to ensure that such programs are preparing teachers who meet the applicable State certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special education teachers, the qualifications described in section 612(a)(14)(C) of the IDEA, are able to understand scientifically valid research, and are able to use advanced technology effectively in the classroom, including use of instructional techniques to improve student academic achievement, by—

(i) Retraining or recruiting faculty; and

(ii) Designing (or redesigning) teacher preparation programs that—

(A) Prepare teachers to serve in low-performing schools and close student achievement gaps, and that are based on rigorous academic content, scientifically valid research (including scientifically based reading research and mathematics research, as it becomes available), and challenging State academic content standards and student academic achievement standards; and

(B) Promote strong teaching skills.

(2) Providing sustained and high-quality preservice clinical experience, including the mentoring of prospective teachers by exemplary teachers, substantially increasing interaction between faculty at IHEs and new and experienced teachers, principals, and other administrators at elementary schools or secondary schools, and providing support, including preparation time, for such interaction.

(3) Developing and implementing initiatives to promote retention of teachers who meet the applicable State

certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special education teachers, the qualifications described in section 612(a)(14)(C) of the IDEA, and highly qualified principals, including minority teachers and principals, including programs that provide—

(i) Teacher or principal mentoring from exemplary teachers or principals, respectively; or

(ii) Induction and support for teachers and principals during their first 3 years of employment as teachers or principals, respectively.

(4) Awarding scholarships based on financial need to help students pay the costs of tuition, room, board, and other expenses of completing a teacher preparation program, not to exceed the cost of attendance.

(5) Disseminating information on effective practices for teacher preparation and successful teacher certification and licensure assessment preparation strategies.

(6) Activities authorized under section 202 of the HEA (20 U.S.C. 1022a).

Program Authority: 20 U.S.C. 1033–1033a.

Note: Projects will be awarded and must be operated in a manner consistent with the nondiscrimination requirements contained in Federal civil rights laws.

Applicable Regulations: (a) The Education Department General Administrative Regulations in 34 CFR parts 75, 77, 79, 82, 84, 86, 97, 98, and 99. (b) The Office of Management and Budget Guidelines to Agencies on Governmentwide Debarment and Suspension (Nonprocurement) in 2 CFR part 180, as adopted and amended as regulations of the Department in 2 CFR part 3485. (c) The Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards in 2 CFR part 200, as adopted and amended as regulations of the Department in 2 CFR part 3474. (d) The 2024 NFP. (e) The Administrative Priorities.

Note: The regulations in 34 CFR part 86 apply to institutions of higher education only.

II. Award Information

Type of Award: Discretionary grant.
Estimated Available Funds: \$15,000,000.

Contingent upon the availability of funds and the quality of applications, we may make additional awards in subsequent years from the list of

unfunded applications from this competition.

Estimated Range of Awards: \$450,000 to \$650,000.

Estimated Average Size of Awards: \$550,000.

Estimated Number of Awards: Up to 27.

Note: The Department is not bound by any estimates in this notice.

Project Period: Up to 60 months.

III. Eligibility Information

1. *Eligible Applicants:* Eligible institutions (as articulated under section 241(1) of the HEA) under the Hawkins Program include—

(i) An IHE that has a qualified teacher preparation program that is—

(A) A part B institution (as defined in section 322 of the HEA);

(B) A Hispanic-serving institution (as defined in section 502 of the HEA);

(C) A Tribal College or University (as defined in section 316 of the HEA);

(D) An Alaska Native-serving institution (as defined in section 317(b) of the HEA);

(E) A Native Hawaiian-serving institution (as defined in section 317(b) of the HEA);

(F) A Predominantly Black Institution (as defined in section 318 of the HEA);

(G) An Asian American and Native American Pacific Islander-serving institution (as defined in section 320(b) of the HEA); or

(H) A Native American-serving, nontribal institution (as defined in section 319 of the HEA);

(ii) A consortium of institutions described in paragraph (i); or

(iii) An institution described in paragraph (i), or a consortium described in paragraph (ii), in partnership with any other IHE, but only if the center of excellence established is located at an institution described in paragraph (i).

Note: A consortium of institutions under this competition must follow the procedures under 34 CFR 75.127–75.129 in developing a group application. This includes developing an agreement that details the activities that each member of the group plans to perform and binds each member of the group to every statement and assurance made by the applicant in the application. This agreement must be submitted with the application.

2. a. *Cost Sharing or Matching:* This competition does not require cost sharing or matching.

b. *Supplement-Not-Supplant:* Grant funds must be used so that they supplement and, to the extent practical, increase the funds that would otherwise be available for the activities to be carried out under this grant. (2024 NFP)

c. *Indirect Cost Rate Information:* A grantee's indirect cost reimbursement is limited to 8 percent of a modified total direct cost base. For more information regarding indirect costs, or to obtain a negotiated indirect cost rate, please see www.ed.gov/about/offices/list/ocfo/intro.html. (2024 NFP)

d. *Administrative Cost Limitation:* In accordance with section 242(e) of the HEA, an eligible institution that receives a grant under this program may use not more than 2 percent of the funds provided to administer the grant. All administrative expenses must be reasonable and necessary and conform to Cost Principles described in 2 CFR part 200 subpart E of the Uniform Guidance.

3. *Subgrantees:* A grantee under this competition may not award subgrants to entities to directly carry out project activities described in its application.

4. *Draft Written Agreement with Clinical Practice Partner(s):* An applicant must provide a Draft Written Agreement (DWA) that identifies the partnership between: (1) at least one eligible IHE with a State accredited teacher preparation program, and (2) a high-need local educational agency (LEA) or consortium of high-need LEAs, or with a high-need school or consortium of high-need schools. The agreement with partners is intended to ensure that the parties joining the project are committed to fulfilling the purpose of the clinical practice by either creating new partnerships or expanding existing partnerships, and that teacher candidates will not become the teacher of record prior to completing the certification program, including pre-service clinical experience, and, for any candidates who entered the program without a bachelor's degree, obtaining a bachelor's. Grantees will finalize the DWA into a Final Written Agreement (FWA) within 120 days of grant award notification. (2024 NFP)

IV. Application and Submission Information

1. *Application Submission Instructions:* Applicants are required to follow the Common Instructions for Applicants to Department of Education Discretionary Grant Programs, published in the **Federal Register** on December 7, 2022 (87 FR 75045), and available at www.federalregister.gov/d/2022-26554, which contain requirements and information on how to submit an application. Please note that these Common Instructions supersede the version published on December 27, 2021.

2. *Intergovernmental Review:* This program is subject to Executive Order

12372 and the regulations in 34 CFR part 79. Information about Intergovernmental Review of Federal Programs under Executive Order 12372 is in the application package for this program.

3. *Funding Restrictions:* We reference regulations outlining funding restrictions in the *Applicable Regulations* section of this notice.

4. *Recommended Page Limit:* The application narrative is where you, the applicant, address the selection criteria that reviewers use to evaluate your application. We recommend that you (1) limit the application narrative to no more than 50 pages and (2) use the following standards:

- A “page” is 8.5” x 11”, on one side only, with 1” margins at the top, bottom, and both sides.
- Double space (no more than three lines per vertical inch) all text in the application narrative, except titles, headings, footnotes, quotations, references, and captions.
- Use a font that is either 12 point or larger or no smaller than 10 pitch (characters per inch).
- Use one of the following fonts: Times New Roman, Courier, Courier New, or Arial.

The recommended page limit does not apply to the cover sheet; the budget section, including the narrative budget justification; the assurances and certifications; or the one-page abstract. However, the recommended page limit does apply to all the application narrative.

V. Application Review Information

1. *Selection Criteria:* The selection criteria for this competition are from 34 CFR 75.210. The points assigned to each criterion are indicated in the parentheses next to the criterion. An applicant may earn up to a total of 100 points based on the selection criteria and up to 10 additional points under the competitive preference priorities, for a total score of up to 110 points. All applications will be evaluated based on the selection criteria as follows:

(a) *Quality of the Project Design.* (Maximum 50 points)

The Secretary considers the quality of the design of the proposed project. In determining the quality of the design of the proposed project, the Secretary considers the following factors:

(1) The extent to which the proposed project is part of a comprehensive effort to improve teaching and learning and support rigorous academic standards for students. (up to 10 points)

(2) The extent to which the design of the proposed project reflects up-to-date

knowledge from research and effective practice. (up to 5 points)

(3) The extent to which the goals, objectives, and outcomes to be achieved by the proposed project are clearly specified and measurable. (up to 5 points)

(4) The extent to which the design of the proposed project is appropriate to, and will successfully address, the needs of the target population or other identified needs. (up to 10 points)

(5) The extent to which the proposed project demonstrates a rationale (as defined in this notice). (up to 10 points)

(6) The extent to which the design for implementing and evaluating the proposed project will result in information to guide possible replication of project activities or strategies, including information about the effectiveness of the approach or strategies employed by the project. (up to 10 points)

(b) *Significance.* (Maximum 20 points)
The Secretary considers the significance of the proposed project. In determining the significance of the proposed project, the Secretary considers the following factors:

(1) The likelihood that the proposed project will result in system change or improvement. (up to 10 points)

(2) The extent to which the results of the proposed project are to be disseminated in ways that will enable others to use the information or strategies. (up to 10 points)

(c) *Quality of the Project Services.* (Maximum 15 points)

The Secretary considers the quality of the services to be provided by the proposed project. In determining the quality of the services to be provided by the proposed project:

(1) The Secretary considers the quality and sufficiency of strategies for ensuring equal access and treatment for eligible project participants who are members of groups that have traditionally been underrepresented based on race, color, national origin, gender, age, or disability. (up to 5 points)

(2) In addition, the Secretary considers the following factors:

(i) The likely impact of the services to be provided by the proposed project on the intended recipients of those services. (up to 5 points)

(ii) The extent to which the services to be provided by the proposed project involve the collaboration of appropriate partners for maximizing the effectiveness of project services. (up to 5 points)

(d) *Quality of the Management Plan.* (Maximum 5 points)

The Secretary considers the quality of the management plan for the proposed

project. In determining the quality of the management plan for the proposed project, the Secretary considers the adequacy of the management plan to achieve the objectives of the proposed project on time and within budget, including clearly defined responsibilities, timelines, and milestones for accomplishing project tasks.

(e) *Quality of the Project Evaluation.* (Maximum 10 points)

The Secretary considers the quality of the evaluation to be conducted of the proposed project. In determining the quality of the evaluation, the Secretary considers the following factors:

(1) The extent to which the evaluation will provide guidance about effective strategies suitable for replication or testing in other settings. (up to 3 points)

(2) The extent to which the methods of evaluation will provide performance feedback and permit periodic assessment of progress toward achieving intended outcomes. (up to 3 points)

(3) The extent to which the methods of evaluation will, if well implemented, produce promising evidence (as defined in this *notice*) about the project's effectiveness. (up to 4 points)

2. *Review and Selection Process:* We remind potential applicants that in reviewing applications in any discretionary grant competition, the Secretary may consider, under 34 CFR 75.217(d)(3), the past performance of the applicant in carrying out a previous award, such as the applicant's use of funds, achievement of project objectives, and compliance with grant conditions. The Secretary may also consider whether the applicant failed to submit a timely performance report or submitted a report of unacceptable quality.

In addition, in making a competitive grant award, the Secretary requires various assurances, including those applicable to Federal civil rights laws that prohibit discrimination in programs or activities receiving Federal financial assistance from the Department (34 CFR 100.4, 104.5, 106.4, 108.8, and 110.23).

The Secretary will select applications for funding in rank order, according to the average score received from the peer review and from the competitive preference priorities addressed by the applicant. If the Secretary has insufficient funding to award multiple applications with the same score, consistent with section 873(d)(2)(A) and (B) of the HEA, in making a selection, the first tiebreaker will be to prioritize applicants from categories of eligible institutions that have been underfunded in this program. If a tie still exists after applying the first tiebreaker, the

Secretary will prioritize under-resourced institutions, such as selecting the applications from institutions with the lowest endowment per FTE. If a third tiebreaker is required, the Secretary will select the applicant with the highest score in the quality of project services selection criterion. Finally, if a fourth tiebreaker is required, the Secretary will select the applicant with the highest score in the quality of project design selection criterion.

3. Risk Assessment and Specific Conditions: Consistent with 2 CFR 200.206, before awarding grants under this competition, the Department conducts a review of the risks posed by applicants. Under 2 CFR 200.208, the Secretary may impose specific conditions and, under 2 CFR 3474.10, in appropriate circumstances, high-risk conditions on a grant if the applicant or grantee is not financially stable; has a history of unsatisfactory performance; has a financial or other management system that does not meet the standards in 2 CFR part 200, subpart D; has not fulfilled the conditions of a prior grant; or is otherwise not responsible.

4. Integrity and Performance System: If you are selected under this competition to receive an award that over the course of the project period may exceed the simplified acquisition threshold (currently \$250,000), under 2 CFR 200.206(a)(2) we must make a judgment about your integrity, business ethics, and record of performance under Federal awards—that is, the risk posed by you as an applicant—before we make an award. In doing so, we must consider any information about you that is in the integrity and performance system (currently referred to as the Federal Awardee Performance and Integrity Information System (FAPIIS)), accessible through the System for Award Management. You may review and comment on any information about yourself that a Federal agency previously entered and that is currently in FAPIIS.

Please note that, if the total value of your currently active grants, cooperative agreements, and procurement contracts from the Federal Government exceeds \$10,000,000, the reporting requirements in 2 CFR part 200, appendix XII, require you to report certain integrity information to FAPIIS semiannually. Please review the requirements in 2 CFR part 200, appendix XII, if this grant plus all the other Federal funds you receive exceed \$10,000,000.

5. In General: In accordance with the Office of Management and Budget's guidance located at 2 CFR part 200, all applicable Federal laws, and relevant

Executive guidance, the Department will review and consider applications for funding pursuant to this notice inviting applications in accordance with—

(a) Selecting recipients most likely to be successful in delivering results based on the program objectives through an objective process of evaluating Federal award applications (2 CFR 200.205);

(b) Prohibiting the purchase of certain telecommunication and video surveillance services or equipment in alignment with section 889 of the National Defense Authorization Act of 2019 (Pub. L. 115–232) (2 CFR 200.216);

(c) Providing a preference, to the extent permitted by law, to maximize use of goods, products, and materials produced in the United States (2 CFR 200.322); and

(d) Terminating agreements in whole or in part to the greatest extent authorized by law if an award no longer effectuates the program goals or agency priorities (2 CFR 200.340).

VI. Award Administration Information

1. Award Notices: If your application is successful, we notify your U.S. Representative and U.S. Senators and send you a Grant Award Notification (GAN); or we may send you an email containing a link to access an electronic version of your GAN. We may notify you informally, also.

If your application is not evaluated or not selected for funding, we notify you.

2. Administrative and National Policy Requirements: We identify administrative and national policy requirements in the application package and reference these and other requirements in the *Applicable Regulations* section of this notice.

We reference the regulations outlining the terms and conditions of an award in the *Applicable Regulations* section of this notice and include these and other specific conditions in the GAN. The GAN also incorporates your approved application as part of your binding commitments under the grant.

3. Open Licensing Requirements: Unless an exception applies, if you are awarded a grant under this competition, you will be required to openly license to the public grant deliverables created in whole, or in part, with Department grant funds. When the deliverable consists of modifications to pre-existing works, the license extends only to those modifications that can be separately identified and only to the extent that open licensing is permitted under the terms of any licenses or other legal restrictions on the use of pre-existing works. Additionally, a grantee or subgrantee that is awarded competitive

grant funds must have a plan to disseminate these public grant deliverables. This dissemination plan can be developed and submitted after your application has been reviewed and selected for funding. For additional information on the open licensing requirements please refer to 2 CFR 3474.20.

4. Reporting: (a) If you apply for a grant under this competition, you must ensure that you have in place the necessary processes and systems to comply with the reporting requirements in 2 CFR part 170 should you receive funding under the competition. This does not apply if you have an exception under 2 CFR 170.110(b).

(b) At the end of your project period, you must submit a final performance report, including financial information, as directed by the Secretary. If you receive a multiyear award, you must submit an annual performance report that provides the most current performance and financial expenditure information as directed by the Secretary under 34 CFR 75.118. The Secretary may also require more frequent performance reports under 34 CFR 75.720(c). For specific requirements on reporting, please go to www.ed.gov/fund/grant/apply/appforms/appforms.html.

(c) Under 34 CFR 75.250(b), the Secretary may provide a grantee with additional funding for data collection analysis and reporting. In this case, the Secretary establishes a data collection period.

5. Performance Measures: For the purposes of Department reporting under 34 CFR 75.110, the Department will use the following performance measures to evaluate the success of the Hawkins Program grants:

(a) The number and percentage of teacher candidates, served by the funded program, who complete the teacher preparation program, disaggregated by race.

(b) The number and percentage of teacher candidates, served by the funded program, disaggregated by race, who become fully certified and are placed as teachers of record in high-need schools or hard-to-staff schools.

(c) The number and percentage of bilingual and/or multilingual teacher candidates, served by the funded program, who complete the teacher preparation program.

(d) The number and percentage of bilingual and/or multilingual teacher candidates, served by the funded program, who become fully certified and are placed as teachers of record in high-need schools or hard-to-staff schools.

(e) The number and percentage of program completers who were employed for the first time as teachers of record in the preceding year by the partner high-need schools or hard-to-staff schools and were retained for the current school year.

(f) The number and percentage of program completers who were employed by the partner high-need school or hard-to-staff school for three consecutive years after initial employment.

(g) The number and percentage of program completers who are employed by the partner high-need school or hard-to-staff school teaching in mathematics, science, bilingual education, special education, career and technical education, or any other field of expertise where the State education agency determines that there is a shortage of qualified teachers.

VII. Other Information

Accessible Format: On request to the program contact person listed under **FOR FURTHER INFORMATION CONTACT**, individuals with disabilities can obtain this document and a copy of the application package in an accessible format.

The Department will provide the requestor with an accessible format that may include Rich Text Format (RTF) or text format (txt), a thumb drive, an MP3 file, braille, large print, audiotape, compact disc, or other accessible format.

Electronic Access to This Document: The official version of this document is the document published in the **Federal Register**. You may access the official edition of the **Federal Register** and the Code of Federal Regulations at www.govinfo.gov. At this site you can view this document, as well as all other documents of this Department published in the **Federal Register**, in text or Portable Document Format (PDF). To use PDF, you must have Adobe Acrobat Reader, which is available free at the site.

You may also access documents of the Department published in the **Federal Register** by using the article search feature at www.federalregister.gov. Specifically, through the advanced search feature at this site, you can limit your search to documents published by the Department.

Nasser Paydar,

Assistant Secretary for Postsecondary Education.

[FR Doc. 2024-07132 Filed 4-3-24; 8:45 am]

BILLING CODE 4000-01-P

DEPARTMENT OF EDUCATION

[Docket No.: ED-2024-SCC-0053]

Agency Information Collection Activities; Comment Request; Evaluation of Transition Supports for Youth With Disabilities

Correction

In notice document 2024-06753, appearing on pages 22133-22134 in the issue of Friday, March 29, 2024, make the following correction:

On page 22133, in the third column, in the **DATES** section, the entry "June 28, 2024" should read "May 28, 2024".

[FR Doc. C1-2024-06753 Filed 4-2-24; 4:15 pm]

BILLING CODE 0099-10-D

DEPARTMENT OF EDUCATION

Applications for New Awards; Teacher Quality Partnership Grant Program

AGENCY: Office of Elementary and Secondary Education, Department of Education.

ACTION: Notice.

SUMMARY: The Department of Education (Department) is issuing a notice inviting applications for fiscal year (FY) 2024 for the Teacher Quality Partnership Grant (TQP) program, Assistance Listing Number 84.336S. This notice relates to the approved information collection under OMB control number 1894-0006.

DATES:

Applications Available: April 4, 2024.

Deadline for notice of intent to apply:

Applicants are strongly encouraged, but not required, to submit a notice of intent to apply by May 6, 2024.

Deadline for transmittal of applications: June 3, 2024.

Deadline for intergovernmental review: August 2, 2024.

Pre-application webinars: The Office of Elementary and Secondary Education intends to post pre-recorded informational webinars designed to provide technical assistance to interested applicants for grants under the TQP program. These informational webinars will be available on the TQP web page shortly after this notice is published in the **Federal Register** at <https://oese.ed.gov/offices/office-of-discretionary-grants-support-services/effective-educator-development-programs/teacher-quality-partnership/applicant-info-and-eligibility>.

ADDRESSES: For the addresses for obtaining and submitting an application, please refer to our Common Instructions for Applicants to Department of Education Discretionary

Grant Programs, published in the **Federal Register** on December 7, 2022 (87 FR 75045) and available at www.federalregister.gov/documents/2022/12/07/2022-26554/common-instructions-for-applicants-to-department-of-education-discretionary-grant-programs.

FOR FURTHER INFORMATION CONTACT: Mia Howerton, U.S. Department of Education, 400 Maryland Avenue SW, Washington, DC 20202-5960. Email: Mia.Howerton@ed.gov or TQPartnership@ed.gov.

If you are deaf, hard of hearing, or have a speech disability and wish to access telecommunications relay services, please dial 7-1-1.

SUPPLEMENTARY INFORMATION:

Full Text of Announcement

I. Funding Opportunity Description

Purpose of Program: The purposes of the TQP program are to improve student achievement; improve the quality of prospective and new teachers by improving the preparation of prospective teachers and enhancing professional development activities for new teachers; hold teacher preparation programs at institutions of higher education (IHEs) accountable for preparing teachers who meet applicable State certification and licensure requirements; and recruit highly qualified individuals, including individuals of color and individuals from other occupations, into the teaching force.

Background: The Department is committed to recruiting, preparing, and retaining racially, culturally, and linguistically diverse educators to the teaching workforce. This commitment includes promoting educator diversity and ensuring that education is a profession that people from all backgrounds can pursue by supporting comprehensive, high-quality and affordable pathways into the profession. The Department thinks preparing, developing and supporting a diverse educator workforce is critical to strengthening student success. Additionally, addressing high-need shortage areas helps to ensure all students have access to a high-quality, well-rounded education. Through Raise the Bar: Lead the World,¹ the Department is working in partnership with States, Tribes, local educational agencies (LEAs), and educator preparation programs, including Historically Black Colleges and

¹ <https://www.ed.gov/raisethebar/eliminating-educator-shortages-compensation-preparation-leadership>.

Universities (HBCUs), Tribally Controlled Colleges and Universities (TCCUs), Hispanic-Serving Institutions (HSIs), and other Minority Serving Institutions (MSIs), to eliminate educator shortages in our nation's schools and to strengthen and diversify the education profession. The priorities used in this FY 2024 TQP competition both highlight and advance the goals of Raise the Bar to ultimately improve student achievement by placing highly qualified, diverse educators in classrooms across the country. The TQP program supports "eligible partnerships" that pair a high-need LEA, a high-need school served by the LEA, or a high-need early childhood education (ECE) program with a partner institution that includes a school, department, or program of education within such partner institution, and a school or department of arts and sciences within such partner institution. Such partnerships also may include certain other entities described below. Under section 202(d) and (e) of the Higher Education Act of 1965, as amended (HEA), these partnerships must implement either (a) teacher preparation programs at the pre baccalaureate or "fifth-year" level that include specific reforms in IHEs' existing teacher preparation programs; or (b) teacher residency programs for individuals who are recent graduates with strong academic backgrounds or are mid-career professionals from outside the field of education.

In this FY 2024 TQP competition, through Absolute Priorities 1 and 2, we support pre-baccalaureate and teacher residency models that would emphasize the creation or expansion of high-quality, comprehensive pathways into the classroom. Through Absolute Priorities 3 and 4, we add a focus on school leadership. Absolute Priority 3 supports the development of school leader programs in conjunction with the preparation of a new pre-baccalaureate model for teachers under Absolute Priority 1. Absolute Priority 4 supports the development of school leader programs in conjunction with a new effective teacher residency model under Absolute Priority 2. Research on the TQP program shows that high-quality residency models can expand the pool of well-prepared applicants entering the teaching profession, promoting diversity of the workforce and bringing a wide range of experiences into the classroom to support students. In addition, the close partnership between school districts and IHEs required by the TQP program ensures that preparation programs are closely aligned with

practice. A 2014 implementation study published by the Institute of Education Sciences shows that residents are more likely than nonresidents to report feeling prepared to enter the classroom, and that after program completion, more than 90 percent of residents stayed in their school district for three years.² High-quality residency programs are a critical part of ensuring that all students have access to well-prepared and qualified educators.

The Department also recognizes that school leaders are an important school-based factor that affects student learning. As described further below, school leaders play a critically important role in students' academic success, especially in underserved schools. School leaders serve as instructional leaders, shaping the schoolwide vision of academic success and creating the learning conditions that support strong teaching and learning, including providing feedback and coaching, creating opportunities for teacher collaboration, and connecting teachers with aligned professional development opportunities. By creating positive working conditions and cultivating enhanced teacher leadership opportunities, school leaders also play a pivotal role in recruiting and retaining highly effective teachers.

A 2021 report entitled "How Principals Affect Students and Schools: A Systematic Synthesis of Two Decades of Research" details how strong principals affect students' educational and social outcomes as well as other outcomes, including teacher retention.³ The report found principals' contributions to student achievement were nearly as large as the average effects of teachers identified in similar studies—but larger in scope because they were distributed over an entire school rather than a single classroom. The report notes that its findings on the importance of principals' effects suggest the need for renewed attention to strategies for cultivating, selecting, preparing, and supporting a high-quality principal workforce.

This competition includes four competitive preference priorities.

² Silva, T., McKie, A., Knechtel, V., Gleason, P., & Makowsky, L. (2014). Teaching Residency Programs: A Multisite Look at a New Model to Prepare Teachers for High-Need Schools (NCEE 2015–4002). Washington, DC: National Center for Education Evaluation and Regional Assistance, Institute of Education Sciences, U.S. Department of Education.

³ Grissom, J.A., Egalite, A.J., and Lindsay, C.A. "How Principals Affect Students and Schools: A Systematic Synthesis of Two Decades of Research," February 2021. www.wallacefoundation.org/knowledgecenter/pages/how-principals-affect-students-and-schools-a-systematic-synthesis-of-two-decades-of-research.aspx.

Competitive Preference Priority 1 is from the Final Priorities—Effective Educator Development (EED) Division, published in the **Federal Register** on July 9, 2021 (86 FR 36217) (EED NFP), and focuses on projects that propose to increase educator diversity. Under Competitive Preference Priority 1, projects must be designed to diversify the teacher pipeline by addressing identified teacher shortage areas in partnership with HBCUs, TCCUs, HSIs, and other MSIs. Teachers of color benefit all students and can have a particularly strong positive impact on students of color.⁴ Today, more than half of K–12 public school students are students of color. The Department recognizes that diverse educators play a critical role in promoting equity in our education system.⁵

Competitive Preference Priorities 2, 3, and 4 are all from the Secretary's Supplemental Priorities and Definitions for Discretionary Grants Programs, published in the **Federal Register** on December 10, 2021 (86 FR 70612) (Supplemental Priorities). Competitive Preference Priority 2 focuses on projects that propose to support a diverse educator workforce that is prepared with the necessary certification and credentialing to teach in shortage areas and high-need schools. Competitive Preference Priority 2 focuses on strengthening teacher recruitment, selection, preparation, support, development, and effectiveness in ways that are consistent with the Department's policy goals of supporting teachers as professionals and improving outcomes for all students, by ensuring that underserved students have equal access to fully qualified, experienced, diverse, and effective educators. There is significant inequity in students' access to fully qualified, experienced, and effective teachers, particularly for students from low-income backgrounds, students of color, and children or students with disabilities.⁶ Teacher candidates deserve access to high-quality comprehensive preparation programs that are aligned with research-based practices, including providing extensive clinical experience, high standards and the necessary supports for successful completion. Additionally,

⁴ https://learningpolicyinstitute.org/sites/default/files/productfiles/Diversifying_Teaching_Profession_REPORT_0.pdf.

⁵ <https://nces.ed.gov/programs/coe/indicator/cge>; and <https://www.bls.gov/cps/cpsaat11.htm>.

⁶ Isenberg, E., Max, J., Gleason, P., Johnson, M., Deutsch, J., and Hansen, M. (2016). Do Low-Income Students Have Equal Access to Effective Teachers? Evidence from 26 Districts (NCEE 2017–4007). Washington, DC: National Center for Education Evaluation and Regional Assistance, Institute of Education Sciences, U.S. Department of Education.

it is crucial to support and retain educators through practices such as mentoring; creating or enhancing opportunities for professional growth, including leadership opportunities; providing competitive compensation; and creating conditions for successful teaching and learning. Finally, Competitive Preference Priority 2 emphasizes the need to increase the number of teachers with certification or dual certification in shortage areas, as well as advanced certifications from nationally recognized professional organizations.

Competitive Preference Priorities 3 and 4 focus on projects that propose to meet students' social, emotional, and academic needs and support projects that propose to promote equity in student access to educational resources and opportunities. These competitive preference priorities recognize the social, emotional, and academic needs of teacher candidates, as well as the importance of preparing those teachers to create inclusive, supportive, equitable, unbiased, and identity-safe learning environments for their students.

Research has demonstrated that, in elementary and secondary schools, children learn, grow, and achieve at higher levels in safe and supportive environments and in the care of responsive adults they can trust.⁷ It is critical, then, to prioritize support for students' social, emotional, and academic needs, not only to benefit students' social and emotional wellness, but also to support their academic success. Mounting evidence suggests that supporting social and emotional learning can contribute to overall student development.⁸ Therefore, educators need to develop skills to effectively incorporate social and emotional learning into their instructional practice.

Lastly, this competition includes two invitation priorities for (1) applicants that propose evidence-based Grow Your

Own (GYO) projects that encourage members of the community to pursue teaching careers, including through registered apprenticeship programs for teachers; and (2) applicants that promote professional development opportunities for teachers of students in grades K–3.

GYO projects can help address teacher shortages by increasing retention rates while also enhancing educator diversity. The Biden Administration is committed to strengthening and diversifying teacher preparation, including by supporting evidence-based residency and GYO programs, which may be provided through a high-quality registered apprenticeship program for teachers, to strengthen teacher pipelines and address shortages, increase the number of teachers of color, and support the growth of teachers.⁹ GYO programs encourage partnerships between LEAs and educator preparation programs to recruit and develop teachers from the communities the school or district serves. The effort to recruit and retain diverse educators, including through GYO programs, starts with such a collaboration. By fostering a shared reliance on the teacher preparation work that both the districts and IHEs provide, GYO models promote the preparation of local residents who will then be retained in that community and help to build capacity. A report from New America that reviewed GYO programs in all 50 states¹⁰ suggests that homegrown teachers have higher rates of retention and GYO programs remove barriers that have kept some individuals from being able to access and persist in an educator preparation program. The Department believes GYO warrants investments through the TQP program for further learning and continued evidence-building, replication, and dissemination. GYO programs may include high school dual-enrollment or early college programs and may be provided through registered apprenticeship programs for teachers.

Registered apprenticeships can be an effective, high-quality “earn and learn” model that allows candidates to earn their teaching credential while earning pay by combining coursework with structured, paid on-the-job learning

experiences with a mentor teacher, combined with coursework and other components of an evidence-based program.¹¹ Registered apprenticeship programs for K–12 teachers can be used to establish, scale, and build on existing high-quality pathways into teaching that emphasize classroom-based experience, such as GYO and teacher residency programs. By reducing the cost of earning a license and offering flexible scheduling, registered apprenticeship programs are designed to open the doors to the profession to those who may otherwise face barriers, including people of color, people from low-income backgrounds, and individuals such as paraprofessionals who may already have decades of experience in the classroom but previously could not afford to become a teacher. Once registered with the U.S. Department of Labor or their State apprenticeship agency (requirements vary by State), these programs can access Federal workforce funding, such as Workforce Innovation and Opportunity Act and Carl D. Perkins Career and Technical Education Act (Perkins V) funding, in addition to other Federal, State, and local education and workforce funds, bringing additional resources to help address educator shortages.

In August of 2022, Secretary Cardona and then-Labor Secretary Marty Walsh issued a joint Dear Colleague Letter¹² calling on all States to establish registered apprenticeship programs for K–12 teachers to help eliminate educator shortages and outlining how States and other interested parties can learn more about this approach.

Applicants are encouraged to explore resources on registered apprenticeship programs for teachers on the Department's Raise the Bar web page on eliminating educator shortages;¹³ at the Department of Labor's apprenticeship website focused on the education industry;¹⁴ and through the resources of the Pathways Alliance, including National Guidelines for Apprenticeship Standards for K–12 Teacher Apprenticeships, approved by the Department of Labor and previously highlighted by the Department, to support high-quality programs.¹⁵

¹¹ <https://www.apprenticeship.gov/apprenticeship-industries/education>.

¹² <https://www.apprenticeship.gov/sites/default/files/22-0119-joint-dcl-signed-ed.pdf>.

¹³ <https://www.ed.gov/raisethebar/educators>.

¹⁴ <https://www.apprenticeship.gov/apprenticeship-industries/education>.

¹⁵ <https://www.thepathwaysalliance.org/reports;https://www.ed.gov/news/press-releases/education-labor-departments-announce-new-efforts-to-advance-teacher-preparation-programs-and-expand-registered-apprenticeships-educators>.

⁷ Reyes, M.R., Brackett, M.A., Rivers, S.E., White, M., & Salovey, P. (2012). Classroom Emotional Climate, Student Engagement, and Academic Achievement. *Journal of Educational Psychology*, 104 (3), 700.

⁸ Cross Francis, D., Liu, J., Bharaj, P.K., & Eker, A. (2019). “Integrating Social-emotional and Academic Development in Teachers' Approaches to Educating Students.” *Policy Insights from the Behavioral and Brain Sciences*, 6 (2), 138–146; Swanson, E., Melguizo, T., & Martorell, P. (2020). *Examining the Relationship between Psychosocial and Academic Outcomes in Higher Education: A Descriptive Analysis*. (EdWorkingPaper: 20–286); Robbins, S.B., Lauver, K., Le, H., Davis, D., Langley, R., & Carlstrom, A. (2004). *Do Psychosocial and Study Skill Factors Predict College Outcomes? A Meta-Analysis*. *Psychological Bulletin*, 130(2), 261–288.

⁹ <https://www.ed.gov/news/press-releases/biden-harris-administration-announces-public-and-private-sector-actions-strengthen-teaching-profession-and-help-schools-fill-vacancies>; <https://ies.ed.gov/ncee/edlabs/regions/northwest/pdf/strategies-for-educators.pdf>.

¹⁰ Garcia, A. (2020). “A 50-State Scan of Grow Your Own Teacher Policies and Programs.” www.newamerica.org/education-policy/reports/grow-your-own-teachers/.

Finally, the Department seeks to strengthen professional development for early elementary educators and school leaders. Given the data on the widening opportunity and achievement gaps for students from low-income backgrounds during the kindergarten year that persists into and through the elementary grades,¹⁶ research suggests that gains in preschool are not sustained in kindergarten after preschool for students from low-income backgrounds,¹⁷ and the importance of students meeting 3rd grade outcomes to support their future success,¹⁸ elementary school leaders and K–2 educators would benefit from targeted professional development, supports, and strategies to ensure more early grade students experience early school success.

Priorities: This notice contains four absolute priorities, four competitive preference priorities, and two invitational priorities. In accordance with 34 CFR 75.105(b)(2)(iv), the absolute priorities are from section 202(d), (e), and (f) of the HEA (20 U.S.C. 1022a(d), (e) and (f)). Competitive Preference Priority 1 is from the EED NFP, and Competitive Preference Priorities 2, 3, and 4 are from the Supplemental Priorities.

Absolute Priorities: For FY 2024 and any subsequent year in which we make awards from the list of unfunded applications from this competition, these priorities are absolute priorities. All applications must address only one of the four absolute priorities. Each of the four absolute priorities constitutes its own funding category. Assuming that applications in each funding category are of sufficient quality, the Secretary intends to award grants under each absolute priority.

Applications will be scored and placed in rank order by absolute priority; thus, applications will be scored and ranked separately by absolute priority to create four funding slates. Applications that address more than one absolute priority or do not

clearly identify the absolute priority being addressed will not be reviewed.

Absolute Priority 1—Partnership Grants for the Preparation of Teachers.

Under this priority, an eligible partnership must carry out an effective pre-baccalaureate teacher preparation program or a fifth-year initial licensing program that includes all of the following:

(a) **Program Accountability.** Implementing reforms, described in paragraph (b) of this priority, within each teacher preparation program and, as applicable, each preparation program for ECE programs, of the eligible partnership that is assisted under this priority, to hold each program accountable for—

(1) **Preparing—**

(i) New or prospective teachers to meet the applicable State certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special education teachers, the qualifications described in section 612(a)(14)(C) of the Individuals with Disabilities Education Act (IDEA) (including teachers in rural school districts, special educators, and teachers of students who are limited English proficient);

(ii) Such teachers and, as applicable, early childhood educators, to understand empirically-based practice and scientifically valid research related to teaching and learning and the applicability of such practice and research, including through the effective use of technology, instructional techniques, and strategies consistent with the principles of universal design for learning, and through positive behavioral interventions and support strategies to improve student achievement; and

(iii) As applicable, early childhood educators to be highly competent; and

(2) **Promoting strong teaching skills** and, as applicable, techniques for early childhood educators to improve children's cognitive, social, emotional, and physical development.

Note: In addressing paragraph (a) of this priority, applicants may either discuss their implementation of reforms within all teacher preparation programs that the partner IHE administers and that would be assisted under this TQP grant, or selected teacher preparation programs that need particular assistance and that would receive the TQP grant funding.

(a) **Required reforms.** The reforms described in paragraph must include—

(1) **Implementing teacher preparation program curriculum changes** that improve, evaluate, and assess how well

all prospective and new teachers develop teaching skills;

(2) **Using empirically-based practice and scientifically valid research**, where applicable, about teaching and learning so that all prospective teachers and, as applicable, early childhood educators—

(i) **Understand and can implement research-based teaching practices** in classroom instruction;

(ii) **Have knowledge of student learning methods;**

(iii) **Possess skills to analyze student academic achievement data and other measures of student learning and use such data and measures to improve classroom instruction;**

(iv) **Possess teaching skills and an understanding of effective instructional strategies across all applicable content areas that enable general education and special education teachers and early childhood educators to—**

(A) **Meet the specific learning needs of all students, including students with disabilities, students who are limited English proficient, students who are gifted and talented, students with low literacy levels, and, as applicable, children in ECE programs; and**

(B) **Differentiate instruction for such students;**

(v) **Can effectively participate as a member of the individualized education program team, as defined in section 614(d)(1)(B) of the IDEA; and**

(vi) **Can successfully employ effective strategies for reading instruction using the essential components of reading instruction;**

(3) **Ensuring collaboration with departments, programs, or units of a partner institution outside of the teacher preparation program in all academic content areas to ensure that prospective teachers receive training in both teaching and relevant content areas in order to meet the applicable State certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special education teachers, the qualifications described in section 612(a)(14)(C) of the IDEA, which may include training in multiple subjects to teach multiple grade levels as may be needed for individuals preparing to teach in rural communities and for individuals preparing to teach students with disabilities;**

(4) **Developing and implementing an induction program;**

(5) **Developing admissions goals and priorities aligned with the hiring objectives of the high-need LEA in the eligible partnership; and**

(6) **Implementing program and curriculum changes, as applicable, to**

¹⁶ James S. Kim, Catherine M. Armstrong, and Thomas Kelley-Kemple. 2017. Practices matter: major findings from the Charlotte-Mecklenburg Schools (CMS) teacher literacy survey. Cambridge, MA: READS Lab, Harvard Graduate School of Education.

¹⁷ Jenkins J.M., Watts T.W., Magnuson K, et al. *High-Quality Kindergarten and First-Grade Classrooms Mitigate Preschool Fadeout?* *J. Res. Educ. Eff.* 2018; 11(3): 339–374.

¹⁸ REL Pacific, “What does the research say about grade 3 reading proficiency as a predictor of future success?” November 1, 2018, <https://ies.ed.gov/ncee/rel/Products/Region/pacific/Ask-A-REL/70038>; Chetty, R. et al., “How Does Your Kindergarten Classroom Affect Your Earnings? Evidence From Project STAR.” NBER Working Paper No. 16381 September 2010, Revised August 2011 JEL No. H0.J0.

ensure that prospective teachers have the requisite content knowledge, preparation, and degree to teach Advanced Placement or International Baccalaureate courses successfully.

(c) Clinical experience and interaction. Developing and improving a sustained and high-quality preservice clinical education program to further develop the teaching skills of all prospective teachers and, as applicable, early childhood educators involved in the program. Such programs must do the following—

(1) Incorporate year-long opportunities for enrichment, including—

(i) Clinical learning in classrooms in high-need schools served by the high need LEA in the eligible partnership, and identified by the eligible partnership; and

(ii) Closely supervised interaction between prospective teachers and faculty, experienced teachers, principals, other administrators, and school leaders at ECE programs (as applicable), elementary schools, or secondary schools, and providing support for such interaction;

(2) Integrate pedagogy and classroom practice and promote effective teaching skills in academic content areas;

(3) Provide high-quality teacher mentoring;

(4) Be offered over the course of a program of teacher preparation;

(5) Be tightly aligned with course work (and may be developed as a fifth year of a teacher preparation program);

(6) Where feasible, allow prospective teachers to learn to teach in the same LEA in which the teachers will work, learning the instructional initiatives and curriculum of that LEA;

(7) As applicable, provide training and experience to enhance the teaching skills of prospective teachers to better prepare such teachers to meet the unique needs of teaching in rural or urban communities; and

(8) Provide support and training for individuals participating in an activity for prospective or new teachers described in this paragraph, paragraphs (a) and (b), or paragraph (d) of this priority, and for individuals who serve as mentors for such teachers, based on each individual's experience. Such support may include—

(i) With respect to a prospective teacher or a mentor, release time for such individual's participation;

(ii) With respect to a faculty member, receiving course workload credit and compensation for time teaching in the eligible partnership's activities; and

(iii) With respect to a mentor, a stipend, which may include bonus,

differential, incentive, or performance pay, based on the mentor's extra skills and responsibilities.

(d) Induction programs for new teachers. Creating an induction program for new teachers or, in the case of an ECE program, providing mentoring or coaching for new early childhood educators.

(e) Support and training for participants in ECE programs. In the case of an eligible partnership focusing on early childhood educator preparation, implementing initiatives that increase compensation for early childhood educators who attain associate or baccalaureate degrees in ECE.

(f) Teacher recruitment. Developing and implementing effective mechanisms (which may include alternative routes to State certification of teachers) to ensure that the eligible partnership is able to recruit qualified individuals to become teachers who meet the applicable State certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special education teachers, the qualifications described in section 612(a)(14)(C) of the IDEA through the activities of the eligible partnership, which may include an emphasis on recruiting into the teaching profession—

(1) Individuals from underrepresented populations;

(2) Individuals to teach in rural communities and teacher shortage areas, including mathematics, science, special education, and the instruction of limited English proficient students; and

(3) Mid-career professionals from other occupations, former military personnel, and recent college graduates with a record of academic distinction.

(g) Literacy training. Strengthening the literacy teaching skills of prospective and, as applicable, new elementary school and secondary school teachers—

(1) To implement literacy programs that incorporate the essential components of reading instruction;

(2) To use screening, diagnostic, formative, and summative assessments to determine students' literacy levels, difficulties, and growth in order to improve classroom instruction and improve student reading and writing skills;

(3) To provide individualized, intensive, and targeted literacy instruction for students with deficiencies in literacy skills; and

(4) To integrate literacy skills in the classroom across subject areas.

Absolute Priority 2—Partnership Grants for the Establishment of Effective Teaching Residency Programs.

(a) In general. Under this priority, an eligible partnership must carry out an effective teaching residency program that includes all of the following activities:

(1) Supporting a teaching residency program described in paragraph II for high-need subjects and areas, as determined by the needs of the high-need LEA in the partnership.

(2) Placing graduates of the teaching residency program in cohorts that facilitate professional collaboration, both among graduates of the teaching residency program and between such graduates and mentor teachers in the receiving school.

(3) Ensuring that teaching residents who participate in the teaching residency program receive—

(i) Effective pre-service preparation as described in paragraph II;

(ii) Teacher mentoring;

(iii) Support required through the induction program as the teaching residents enter the classroom as new teachers; and

(iv) The preparation described below:

(A) Incorporate year-long opportunities for enrichment, including—

(1) Clinical learning in classrooms in high-need schools served by the high-need LEA in the eligible partnership, and identified by the eligible partnership; and

(2) Closely supervised interaction between prospective teachers and faculty, experienced teachers, principals, other administrators, and school leaders at ECE programs (as applicable), elementary schools, or secondary schools, and providing support for such interaction.

(B) Integrate pedagogy and classroom practice and promote effective teaching skills in academic content areas.

(C) Provide high-quality teacher mentoring.

(b) Teaching Residency Programs.

(1) Establishment and design. A teaching residency program under this priority is a program based upon models of successful teaching residencies that serves as a mechanism to prepare teachers for success in the high-need schools in the eligible partnership and must be designed to include the following characteristics of successful programs:

(i) The integration of pedagogy, classroom practice, and teacher mentoring.

(ii) Engagement of teaching residents in rigorous graduate-level course work leading to a master's degree while

undertaking a guided teaching apprenticeship.

(iii) Experience and learning opportunities alongside a trained and experienced mentor teacher—

(A) Whose teaching must complement the residency program so that classroom clinical practice is tightly aligned with coursework;

(B) Who must have extra responsibilities as a teacher leader of the teaching residency program, as a mentor for residents, and as a teacher coach during the induction program for new teachers; and for establishing, within the program, a learning community in which all individuals are expected to continually improve their capacity to advance student learning; and

(C) Who may be relieved from teaching duties as a result of such additional responsibilities.

(iv) The establishment of clear criteria for the selection of mentor teachers based on measures of teacher effectiveness and the appropriate subject area knowledge. Evaluation of teacher effectiveness must be based on, but not limited to, observations of the following—

(A) Planning and preparation, including demonstrated knowledge of content, pedagogy, and assessment, including the use of formative and diagnostic assessments to improve student learning.

(B) Appropriate instruction that engages students with different learning styles.

(C) Collaboration with colleagues to improve instruction.

(D) Analysis of gains in student learning, based on multiple measures that are valid and reliable and that, when feasible, may include valid, reliable, and objective measures of the influence of teachers on the rate of student academic progress.

(E) In the case of mentor candidates who will be mentoring new or prospective literacy and mathematics coaches or instructors, appropriate skills in the essential components of reading instruction, teacher training in literacy instructional strategies across core subject areas, and teacher training in mathematics instructional strategies, as appropriate.

(v) Grouping of teaching residents in cohorts to facilitate professional collaboration among such residents.

(vi) The development of admissions goals and priorities—

(A) That are aligned with the hiring objectives of the LEA partnering with the program, as well as the instructional initiatives and curriculum of such agency, in exchange for a commitment by such agency to hire qualified

graduates from the teaching residency program; and

(B) Which may include consideration of applicants who reflect the communities in which they will teach as well as consideration of individuals from underrepresented populations in the teaching profession.

(vii) Support for residents, once the teaching residents are hired as teachers of record, through an induction program, professional development, and networking opportunities to support the residents through not less than the residents' first two years of teaching.

(2) Selection of individuals as teacher residents.

(i) Eligible individual. In order to be eligible to be a teacher resident in a teaching residency program under this priority, an individual must—

(A) Be a recent graduate of a four-year IHE or a mid-career professional from outside the field of education possessing strong content knowledge or a record of professional accomplishment; and

(B) Submit an application to the teaching residency program.

(ii) Selection criteria for teaching residency program. An eligible

partnership carrying out a teaching residency program under this priority must establish criteria for the selection of eligible individuals to participate in the teaching residency program based on the following characteristics—

(A) Strong content knowledge or record of accomplishment in the field or subject area to be taught.

(B) Strong verbal and written communication skills, which may be demonstrated by performance on appropriate tests.

(C) Other attributes linked to effective teaching, which may be determined by interviews or performance assessments, as specified by the eligible partnership.

(3) Stipends or salaries; applications; agreements; repayments.

(i) Stipends or salaries. A teaching residency program under this priority must provide a one-year living stipend or salary to teaching residents during the teaching residency program.

(ii) Applications for stipends or salaries. Each teacher residency candidate desiring a stipend or salary during the period of residency must submit an application to the eligible partnership at such time, and containing such information and assurances, as the eligible partnership may require.

(iii) Agreements to serve. Each application submitted under paragraph (b)(3)(ii) of this priority must contain or be accompanied by an agreement that the applicant will—

(A) Serve as a full-time teacher for a total of not less than three academic

years immediately after successfully completing the teaching residency program;

(B) Fulfill the requirement under paragraph (b)(3)(iii)(A) of this priority by teaching in a high-need school served by the high-need LEA in the eligible partnership and teach a subject or area that is designated as high need by the partnership;

(C) Provide to the eligible partnership a certificate, from the chief administrative officer of the LEA in which the resident is employed, of the employment required under paragraph (b)(3)(iii)(A) and (B) of this priority at the beginning of, and upon completion of, each year or partial year of service;

(D) Meet the applicable State certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special education teachers, the qualifications described in section 612(a)(14)(C) of the IDEA, when the applicant begins to fulfill the service obligation under paragraph (b)(3)(iii) of this priority; and

(E) Comply with the requirements set by the eligible partnership under paragraph (b)(4) of this priority if the applicant is unable or unwilling to complete the service obligation required by paragraph (b)(3)(iii) of this priority.

(4) Repayments.

(i) In general. A grantee carrying out a teaching residency program under this priority must require a recipient of a stipend or salary under paragraph (b)(3)(i) of this priority who does not complete, or who notifies the partnership that the recipient intends not to complete, the service obligation required by paragraph (b)(3)(iii) of this priority to repay such stipend or salary to the eligible partnership, together with interest, at a rate specified by the partnership in the agreement, and in accordance with such other terms and conditions specified by the eligible partnership, as necessary.

(ii) Other terms and conditions. Any other terms and conditions specified by the eligible partnership may include reasonable provisions for pro-rata repayment of the stipend or salary described in paragraph (b)(3)(i) of this priority or for deferral of a teaching resident's service obligation required by paragraph (b)(3)(iii) of this priority, on grounds of health, incapacitation, inability to secure employment in a school served by the eligible partnership, being called to active duty in the Armed Forces of the United States, or other extraordinary circumstances.

(iii) Use of repayments. An eligible partnership must use any repayment received under paragraph (b)(4) of this priority to carry out additional activities that are consistent with the purpose of this priority.

Absolute Priority 3—Partnership Grants for the Development of Leadership Programs in Conjunction With the Preparation of a Pre-Baccalaureate Model for Teachers.

Under this priority the Secretary gives priority to applications from eligible partnerships that propose to carry out an effective school leadership program that will prepare individuals enrolled or preparing to enroll in such program for careers as superintendents, principals, ECE program directors, or other school leaders (including individuals preparing to work in LEAs located in rural areas who may perform multiple duties in addition to the role of a school leader). An eligible partnership may carry out the school leadership program either in the partner high-need LEA or in further partnership with an LEA located in a rural area. The school leadership program carried out under this priority must include the following activities:

(a) Preparation of school leaders. In preparing school leaders, the school leadership program must include the following activities:

(1) Promoting strong leadership skills and, as applicable, techniques for school leaders to effectively—

(i) Create and maintain a data-driven, professional learning community within the leader's schools;

(ii) Provide a climate conducive to the professional development of teachers, with a focus on improving student achievement and the development of effective instructional leadership skills;

(iii) Understand the teaching and assessment skills needed to support successful classroom instruction and to use data to evaluate teacher instruction and drive teacher and student learning;

(iv) Manage resources and school time to improve student academic achievement and ensure the school environment is safe;

(v) Engage and involve parents, community members, the LEA, businesses, and other community leaders, to leverage additional resources to improve student academic achievement; and

(vi) Understand how students learn and develop in order to increase academic achievement for all students.

(2) Developing and improving a sustained and high-quality preservice clinical education program to further develop the leadership skills of all prospective school leaders involved in

the program. This clinical education program must do the following:

(i) Incorporate year-long opportunities for enrichment, including—

(A) Clinical learning in high-need schools served by the high-need LEA or an LEA located in a rural area in the eligible partnership and identified by the eligible partnership; and

(B) Closely supervised interaction between prospective school leaders and faculty, new and experienced teachers, and new and experienced school leaders, in those high-need schools.

(ii) Integrate pedagogy and practice and promote effective leadership skills, meeting the unique needs of urban, rural, or geographically isolated communities, as applicable.

(iii) Provide for mentoring of new school leaders.

(3) Creating an induction program for new school leaders.

(4) Ensuring that individuals who participate in the school leadership program receive—

(i) Effective preservice preparation as described in paragraph (a)(2) of this priority;

(ii) Mentoring; and

(iii) If applicable, full State certification or licensure to become a school leader.

(5) Developing and implementing effective mechanisms to ensure that the eligible partnership is able to recruit qualified individuals to become school leaders through activities that may include an emphasis on recruiting into school leadership professions—

(i) Individuals from underrepresented populations;

(ii) Individuals to serve as superintendents, principals, or other school administrators in rural and geographically isolated communities and school leader shortage areas; and

(iii) Mid-career professionals from other occupations, former military personnel, and recent college graduates with a record of academic distinction.

(b) In order to be eligible for the school leadership program under this priority, an individual must be enrolled in or preparing to enroll in an IHE, and must—

(1) Be a—

(i) Recent graduate of an IHE;

(ii) Mid-career professional from outside the field of education with strong content knowledge or a record of professional accomplishment;

(iii) Current teacher who is interested in becoming a school leader; or

(iv) School leader who is interested in becoming a superintendent; and

(2) Submit an application to the leadership program.

Note: The leadership program described above must be implemented

in conjunction with a Pre-Baccalaureate Model for Teachers (see Absolute Priority 1). Both a Pre-Baccalaureate Model and a Leadership Model must be proposed for implementation in the application when addressing Absolute Priority 3.

Absolute Priority 4—Partnership Grants for the Development of Leadership Programs in Conjunction With the Establishment of an Effective Teaching Residency Program.

Under this priority the Secretary gives priority to applications from eligible partnerships that propose to carry out an effective school leadership program that will prepare individuals enrolled or preparing to enroll in those programs for careers as superintendents, principals, ECE program directors, or other school leaders (including individuals preparing to work in LEAs located in rural areas who may perform multiple duties in addition to the role of a school leader). An eligible partnership may carry out the school leadership program either in the partner high-need LEA or in further partnership with an LEA located in a rural area. The school leadership program carried out under this priority must include the following activities:

(a) Preparation of school leaders. In preparing school leaders, the school leadership program must include the following activities:

(1) Promoting strong leadership skills and, as applicable, techniques for school leaders to effectively—

(i) Create and maintain a data-driven, professional learning community within the leader's schools.

(ii) Provide a climate conducive to the professional development of teachers, with a focus on improving student achievement and the development of effective instructional leadership skills;

(iii) Understand the teaching and assessment skills needed to support successful classroom instruction and to use data to evaluate teacher and drive teacher and student learning;

(iv) Manage resources and school time to improve student academic achievement and ensure a safe school environment;

(v) Engage and involve parents, community members, the LEA, businesses, and other community leaders, to leverage additional resources to improve student academic achievement; and

(vi) Understand how students learn and develop in order to increase academic achievement for all students.

(2) Developing and improving a sustained and high-quality preservice clinical education program to further develop the leadership skills of all prospective school leaders involved in

the program. This clinical education program must do the following:

(i) Incorporate year-long opportunities for enrichment, including—

(A) Clinical learning in high-need schools served by the high-need LEA or an LEA located in a rural area in the eligible partnership and identified by the eligible partnership; and

(B) Closely supervised interaction between prospective school leaders and faculty, new and experienced teachers, and new and experienced school leaders, in those high-need schools.

(ii) Integrate pedagogy and practice and promote effective leadership skills, meeting the unique needs of urban, rural, or geographically isolated communities, as applicable.

(iii) Provide for mentoring of new school leaders.

(3) Creating an induction program for new school leaders.

(4) Ensuring that individuals who participate in the school leadership program receive—

(i) Effective preservice preparation as described in paragraph (a)(2) of this priority.

(ii) Mentoring; and

(iii) If applicable, full State certification or licensure to become a school leader.

(5) Developing and implementing effective mechanisms to ensure that the eligible partnership is able to recruit qualified individuals to become school leaders through activities that may include an emphasis on recruiting into school leadership professions—

(i) Individuals from underrepresented populations.

(ii) Individuals to serve as superintendents, principals, or other school administrators in rural and geographically isolated communities and school leader shortage areas; and

(iii) Mid-career professionals from other occupations, former military personnel, and recent college graduates with a record of academic distinction.

(b) In order to be eligible for the school leadership program under this priority, an individual must be enrolled in or preparing to enroll in an IHE, and must—

(1) Be a—

(i) Recent graduate of an IHE;

(ii) Mid-career professional from outside the field of education with strong content knowledge or a record of professional accomplishment;

(iii) Current teacher who is interested in becoming a school leader; or

(iv) School leader who is interested in becoming a superintendent; and

(2) Submit an application to the leadership program.

Note: The leadership program described above must be implemented

in conjunction with a Teaching Residency Program (see Absolute Priority 2). Both a Residency Model and a Leadership Model must be proposed for implementation in the application when addressing Absolute Priority 4.

Competitive Preference Priorities: For FY 2024 and any subsequent year in which we make awards from the list of unfunded applications from this competition, these priorities are competitive preference priorities. Under 34 CFR 75.105(c)(2)(i), we award up to an additional four points to an application depending on how well the application addresses Competitive Preference Priority 1, up to an additional three points to an application depending on how well the application addresses Competitive Preference Priority 2, up to an additional two points to an application depending on how well the application addresses Competitive Preference Priority 3, and up to an additional two points to an application depending on how well the application addresses Competitive Preference Priority 4, for a maximum of eleven additional competitive preference points.

If an applicant chooses to address one or more of the competitive preference priorities, the project narrative section of its application must identify its response to the competitive preference priorities it chooses to address.

These priorities are:

Competitive Preference Priority 1—Increasing Educator Diversity (up to 4 points).

Under this priority, applicants must develop projects that are designed to improve the recruitment, outreach, preparation, support, development, and retention of a diverse educator workforce through adopting, implementing, or expanding one or both of the following:

(a) High-quality, comprehensive teacher preparation programs in Historically Black Colleges and Universities (eligible institutions under part B of title III and subpart 4 of part A title VII of the HEA), Hispanic Serving Institutions (eligible institutions under section 502 of the HEA), Tribal Colleges and Universities (eligible institutions under section 316 of the HEA), or other Minority Serving Institutions (eligible institutions under title III and title V of the HEA) that include one year of high-quality clinical experiences (prior to becoming the teacher of record) in high-need schools (as defined in this notice) and that incorporate best practices for attracting, supporting, graduating, and placing underrepresented teacher candidates.

(b) Reforms to teacher preparation programs to improve the diversity of teacher candidates, including changes to ensure underrepresented teacher candidates are fully represented in program admission, completion, placement, and retention as educators.

Competitive Preference Priority 2—Supporting a Diverse Educator Workforce and Professional Growth To Strengthen Student Learning (up to 3 points).

Projects that are designed to increase the proportion of well-prepared, diverse, and effective educators serving students, with a focus on underserved students, through increasing the number of teachers with certification or dual certification in a shortage area, or advanced certifications from nationally recognized professional organizations.

Competitive Preference Priority 3—Meeting Student Social, Emotional, and Academic Needs (up to 2 points).

Projects that are designed to improve students' social, emotional, academic, and career development, with a focus on underserved students, through creating a positive, inclusive, and identity-safe climate at institutions of higher education, through one or more of the following activities:

(a) Fostering a sense of belonging and inclusion for underserved students.

(b) Implementing evidence-based practices for advancing student success for underserved students.

Competitive Preference Priority 4—Promoting Equity in Student Access to Educational Resources and Opportunities (up to 2 points).

Under this priority, an applicant must demonstrate that the applicant proposes a project designed to promote educational equity and adequacy in resources and opportunity for underserved students—

(a) In one or more of the following educational settings:

(1) Early learning programs.

(2) Elementary school.

(3) Middle school.

(4) High school.

(5) Career and technical education programs.

(6) Out-of-school-time settings.

(7) Alternative schools and programs.

(b) That examines the sources of inequity and inadequacy and implements responses, and that may include pedagogical practices in educator preparation programs and professional development programs that are inclusive with regard to race, ethnicity, culture, language, and disability status so that educators are better prepared to create inclusive, supportive, equitable, unbiased, and identity-safe learning environments for their students.

Invitational Priorities: For FY 2024 and any subsequent year in which we make awards from the list of unfunded applications from this competition, these priorities are invitational priorities. Under 34 CFR 75.105(c)(1) we do not give an application that meets one or more of these invitational priorities a competitive or absolute preference over other applications.

These priorities are:

Invitational Priority 1—Partnership Grants for the Establishment of GYO Programs and Registered Apprenticeship Programs for K–12 Teachers.

Projects that establish or scale evidence-based and high quality GYO programs, including through a registered apprenticeship programs, that are designed to address shortages of teachers in high-need areas, schools, and/or geographic areas, or shortages of school leaders in high-need schools, and increase the diversity of qualified individuals entering the teacher, principal, or other school leader workforce, by recruiting and developing teacher candidates from the communities the school or district serves. GYO programs must minimize or eliminate the cost of certification for teacher candidates and compensate educators for clinical experience in classrooms that is part of their certification program. Participants must not become the teacher of record prior to meeting full-state certification requirements. Projects may also include high school dual enrollment and early college opportunities and high-quality registered teacher apprenticeship programs.

A project implementing a new or enhanced GYO program, including through a registered apprenticeship programs, must:

(a) Be developed with the partner LEA to address the needs of its students and teachers;

(b) Use data-driven strategies and evidence-based approaches to increase recruitment, successful completion, and retention of teachers supported by the project;

(c) Provide standards for participants to enter into and complete the program;

(d) Be aligned to evidence-based practices for effective educator preparation, and include practice-based learning opportunities linked to coursework that address state requirements for certification, professional standards for teacher preparation, culturally and linguistically sustaining pedagogies, and the established knowledge base for

education, including the science of learning and development;¹⁹

(e) Have little to no financial burden for program participants, or provide for loan forgiveness;

(f) Require completion of a bachelor's degree either before entering or as a result of the certification program;

(g) Result in the satisfaction of all requirements for full state teacher licensure or certification, excluding emergency, temporary, provisional or other sub-standard licensure or certification; and

(h) Provide increasing levels of responsibility for the resident/GYO participant/apprentice during at least one year of paid on-the-job learning/clinical experience, during which a mentor teacher is the teacher of record.

Invitational Priority 2—Supporting Early Elementary Educators and School Leaders.

Projects that include professional development programs, professional learning communities, and peer learning collaboratives to support elementary educators and school leaders in meeting the wide range of developmental strengths, needs, and experiences of students at kindergarten entry through the early grades with a focus on one or more of the following strategies:

(a) Intentional collaboration for systemic alignment for continuity of services, supports, instruction, relationships, and data sharing across K–2;

(b) Effective and intentional transitions into kindergarten and through the early grades;

(c) Instruction informed by child development and developmentally informed practices;

(d) Partnerships with parents, families and caregivers to allow successful family engagement and everyday school attendance.

Definitions: The definitions for “arts and sciences,” “children from low income families,” “early childhood educator,” “essential components of reading instruction,” “exemplary teacher,” “high-need early childhood education (ECE) program,” “high-need local educational agency (LEA),” “high-need school,” “highly competent,” “induction program,” “limited English proficient,” “partner institution,” “principles of scientific research,” “scientifically valid research,” “teacher mentoring,” “teaching residency program,” and “teaching skills” are

¹⁹ See, for example, for registered apprenticeship programs for teachers, the *National Guidelines for Apprenticeship Standards for K–12 Teacher Apprenticeships*, drafted by the Pathways Alliance and approved by the U.S. Department of Labor <https://www.thepathwaysalliance.org/reports>.

from section 200 of the HEA (20 U.S.C. 1021). The definition of “charter school” is from section 4310(2) of the ESEA (20 U.S.C. 7221i). The definitions of “educational service agency,” “parent,” and “professional development” are from section 8101 of the ESEA (20 U.S.C. 7801). The definitions of “demonstrates a rationale,” “evidence-based,” “experimental study,” “logic model,” “moderate evidence,” “project component,” “promising evidence,” “quasi-experimental design study,” “relevant outcome,” “strong evidence,” and “What Works Clearinghouse Handbooks (WWC Handbooks)” are from 34 CFR 77.1. The definitions of “children or students with disabilities,” “disconnected youth,” “early learning,” “educator,” “military- or veteran connected student,” and “underserved student” are from the Supplemental Priorities.

Arts and sciences means—

(1) When referring to an organizational unit of an IHE, any academic unit that offers one or more academic majors in disciplines or content areas corresponding to the academic subject matter areas in which teachers provide instruction; and

(2) When referring to a specific academic subject area, the disciplines or content areas in which academic majors are offered by the arts and sciences organizational unit.

Charter school means a public school that—

(1) In accordance with a specific State statute authorizing the granting of charters to schools, is exempt from significant State or local rules that inhibit the flexible operation and management of public schools, but not from any rules relating to the other requirements of this definition;

(2) Is created by a developer as a public school, or is adapted by a developer from an existing public school, and is operated under public supervision and direction;

(3) Operates in pursuit of a specific set of educational objectives determined by the school's developer and agreed to by the authorized public chartering agency;

(4) Provides a program of elementary or secondary education, or both;

(5) Is nonsectarian in its programs, admissions policies, employment practices, and all other operations, and is not affiliated with a sectarian school or religious institution;

(6) Does not charge tuition;

(7) Complies with the Age Discrimination Act of 1975 (42 U.S.C. 6101 *et seq.*), title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d *et seq.*),

title IX of the Education Amendments of 1972 (20 U.S.C. 1681 *et seq.*), section 504 of the Rehabilitation Act of 1973 (29 U.S.C. 794), the Americans with Disabilities Act of 1990 (42 U.S.C. 12101 *et seq.*), 20 U.S.C. 1232g (commonly referred to as the “Family Educational Rights and Privacy Act of 1974”), and part B of the IDEA (20 U.S.C. 1411 *et seq.*);

(8) Is a school to which parents choose to send their children, and that—

(i) Admits students on the basis of a lottery, consistent with 20 U.S.C. 7221b(c)(3)(A) if more students apply for admission than can be accommodated; or

(ii) In the case of a school that has an affiliated charter school (such as a school that is part of the same network of schools), automatically enrolls students who are enrolled in the immediate prior grade level of the affiliated charter school and, for any additional student openings or student openings created through regular attrition in student enrollment in the affiliated charter school and the enrolling school, admits students on the basis of a lottery as described in clause (i);

(9) Agrees to comply with the same Federal and State audit requirements as do other elementary schools and secondary schools in the State, unless such State audit requirements are waived by the State;

(10) Meets all applicable Federal, State, and local health and safety requirements;

(11) Operates in accordance with State law;

(12) Has a written performance contract with the authorized public chartering agency in the State that includes a description of how student performance will be measured in charter schools pursuant to State assessments that are required of other schools and pursuant to any other assessments mutually agreeable to the authorized public chartering agency and the charter school; and

(13) May serve students in early childhood education programs or postsecondary students.

Note: Under section 4310(1), the term “authorized public chartering agency” means a “State educational agency, local educational agency, or other public entity that has the authority pursuant to State law and approved by the Secretary [of Education] to authorize or approve a charter school.”

Children from low-income families means children described in section 1124(c)(1)(A) of the Elementary and Secondary Education Act of 1965.

Demonstrates a rationale means a key project component included in the project’s logic model is informed by research or evaluation findings that suggest the project component is likely to improve relevant outcomes.

Disconnected youth means an individual, between the ages 14 and 24, who may be from a low-income background, experiences homelessness, is in foster care, is involved in the justice system, or is not working or not enrolled in (or at risk of dropping out of) an educational institution.

Early childhood educator means an individual with primary responsibility for the education of children in an ECE program.

Early learning means any (a) State licensed or State-regulated program or provider, regardless of setting or funding source, that provides early care and education for children from birth to kindergarten entry, including, but not limited to, any program operated by a child care center or in a family child care home; (b) program funded by the Federal Government or State or local educational agencies (including any IDEA-funded program); (c) Early Head Start and Head Start program; (d) non-relative child care provider who is not otherwise regulated by the State and who regularly cares for two or more unrelated children for a fee in a provider setting; and (e) other program that may deliver early learning and development services in a child’s home, such as the Maternal, Infant, and Early Childhood Home Visiting Program; Early Head Start; and Part C of IDEA.

Educational service agency means a regional public multiservice agency authorized by State statute to develop, manage, and provide services or programs to LEAs.

Educator means an individual who is an early learning educator, teacher, principal or other school leader, specialized instructional support personnel (e.g., school psychologist, counselor, school social worker, early intervention service personnel), paraprofessional, or faculty.

Essential components of reading instruction means explicit and systematic instruction in—

- (1) Phonemic awareness;
- (2) Phonics;
- (3) Vocabulary development;
- (4) Reading fluency, including oral reading skills; and
- (5) Reading comprehension strategies.

Evidence-based means the proposed project component is supported by one or more of strong evidence, moderate evidence, promising evidence, or evidence that demonstrates a rationale.

Exemplary teacher means a teacher who—

(1) Is a highly qualified teacher such as a master teacher;

(2) Has been teaching for at least five years in a public or private school or IHE;

(3) Is recommended to be an exemplary teacher by administrators and other teachers who are knowledgeable about the individual’s performance;

(4) Is currently teaching and based in a public school; and

(5) Assists other teachers in improving instructional strategies, improves the skills of other teachers, performs teacher mentoring, develops curricula, and offers other professional development.

Experimental study means a study that is designed to compare outcomes between two groups of individuals (such as students) that are otherwise equivalent except for their assignment to either a treatment group receiving a project component or a control group that does not. Randomized controlled trials, regression discontinuity design studies, and single-case design studies are the specific types of experimental studies that, depending on their design and implementation (e.g., sample attrition in randomized controlled trials and regression discontinuity design studies), can meet What Works Clearinghouse (WWC) standards without reservations as described in the WWC Handbooks:

(1) A randomized controlled trial employs random assignment of, for example, students, teachers, classrooms, or schools to receive the project component being evaluated (the treatment group) or not to receive the project component (the control group).

(2) A regression discontinuity design study assigns the project component being evaluated using a measured variable (e.g., assigning students reading below a cutoff score to tutoring or developmental education classes) and controls for that variable in the analysis of outcomes.

(3) A single-case design study uses observations of a single case (e.g., a student eligible for a behavioral intervention) over time in the absence and presence of a controlled treatment manipulation to determine whether the outcome is systematically related to the treatment.

High-need early childhood education (ECE) program means an ECE program serving children from low-income families that is located within the geographic area served by a high-need LEA.

High-need local educational agency (LEA) means an LEA—

- (1)(i) For which not less than 20 percent of the children served by the agency are children from low-income families;
 - (ii) That serves not fewer than 10,000 children from low-income families;
 - (iii) That meets the eligibility requirements for funding under the Small, Rural School Achievement program under section 5211(b) of the ESEA; or
 - (iv) That meets eligibility requirements for funding under the Rural and Low-Income School program under section 5221(b) of the ESEA (20 U.S.C. 7351(b)); and—
 - (2)(i) For which there is a high percentage of teachers not teaching in the academic subject areas or grade levels in which the teachers were trained to teach; or
 - (ii) For which there is a high teacher turnover rate or a high percentage of teachers with emergency, provisional, or temporary certification or licensure.
- Note:* Information on how an applicant may demonstrate that a partner LEA meets this definition is included in the application package.
- High-need school* means a school that, based on the most recent data available, meets one or both of the following: (1) The school is in the highest quartile of schools in a ranking of all schools served by an LEA, ranked in descending order by percentage of students from low-income families enrolled in such schools, as determined by the LEA based on one of the following measures of poverty:
- (i) The percentage of students aged 5 through 17 in poverty counted in the most recent census data approved by the Secretary.
 - (ii) The percentage of students eligible for a free or reduced-price school lunch under the Richard B. Russell National School Lunch Act.
 - (iii) The percentage of students in families receiving assistance under the State program funded under part A of title IV of the Social Security Act.
 - (iv) The percentage of students eligible to receive medical assistance under the Medicaid program.
 - (v) A composite of two or more of the measures described in paragraphs (1)(i) through (1)(iv) of this priority.
- (2) In the case of—
 - (i) An elementary school, the school serves students not less than 60 percent of whom are eligible for a free or reduced-price school lunch under the Richard B. Russell National School Lunch Act; or
 - (ii) Any other school that is not an elementary school, the other school

serves students not less than 45 percent of whom are eligible for a free or reduced-price school lunch under the Richard B. Russell National School Lunch Act.

(3) The Secretary may, upon approval of an application submitted by an eligible partnership seeking a grant under title II of the HEA, designate a school that does not qualify as a high-need school under this definition, as a high-need school for the purpose of this competition. The Secretary must base the approval of an application for designation of a school under this clause on a consideration of the information required under section 200(11)(B)(ii) of the HEA and may also take into account other information submitted by the eligible partnership.

Note: Information on how an applicant may demonstrate that a partner school meets this definition is included in the application package.

Highly competent, when used with respect to an early childhood educator, means an educator—

- (1) With specialized education and training in development and education of young children from birth until entry into kindergarten;
- (2) With—
 - (i) A baccalaureate degree in an academic major in the arts and sciences; or
 - (ii) An associate's degree in a related educational area; and
- (3) Who has demonstrated a high level of knowledge and use of content and pedagogy in the relevant areas associated with quality early childhood education.

Induction program means a formalized program for new teachers during not less than the teachers' first two years of teaching that is designed to provide support for and improve the professional performance and advance the retention in the teaching field of, beginning teachers. Such program must promote effective teaching skills and must include the following components:

- (1) High-quality teacher mentoring.
- (2) Periodic, structured time for collaboration with teachers in the same department or field, including mentor teachers, as well as time for information-sharing among teachers, principals, administrators, other appropriate instructional staff, and participating faculty in the partner institution.
- (3) The application of empirically-based practice and scientifically valid research on instructional practices.
- (4) Opportunities for new teachers to draw directly on the expertise of teacher mentors, faculty, and researchers to support the integration of empirically-

based practice and scientifically valid research with practice.

(5) The development of skills in instructional and behavioral interventions derived from empirically-based practice and, where applicable, scientifically valid research.

(6) Faculty who—

(i) Model the integration of research and practice in the classroom; and

(ii) Assist new teachers with the effective use and integration of technology in the classroom.

(7) Interdisciplinary collaboration among exemplary teachers, faculty, researchers, and other staff who prepare new teachers with respect to the learning process and the assessment of learning.

(8) Assistance with the understanding of data, particularly student achievement data, and the applicability of such data in classroom instruction.

(9) Regular and structured observation and evaluation of new teachers by multiple evaluators, using valid and reliable measures of teaching skills.

Limited English proficient,²⁰ when used with respect to an individual, means an individual—

- (1) Who is aged 3 through 21;
- (2) Who is enrolled or preparing to enroll in an elementary school or secondary school;
- (3)(i) Who was not born in the United States or whose native language is a language other than English;
- (ii)(A) Who is a Native American or Alaska Native, or a native resident of the outlying areas; and
- (B) Who comes from an environment where a language other than English has had a significant impact on the individual's level of English language proficiency; or
- (iii) Who is migratory, whose native language is a language other than English, and who comes from an environment where a language other than English is dominant; and
- (4) Whose difficulties in speaking, reading, writing, or understanding the English language may be sufficient to deny the individual—

(i) The ability to meet the challenging State academic standards;

(ii) The ability to successfully achieve in classrooms where the language of instruction is English; or

(iii) The opportunity to participate fully in society.

Logic model (also referred to as a theory of action) means a framework that identifies key project components

- (i) The ability to meet the challenging State academic standards;
- (ii) The ability to successfully achieve in classrooms where the language of instruction is English; or
- (iii) The opportunity to participate fully in society.

Logic model (also referred to as a theory of action) means a framework that identifies key project components

²⁰The HEA definition of "limited English proficient" cross-references a definition of "English learner" in section 8101 of the ESEA. Because the HEA is the source of funding for this program, we use the HEA term "limited English proficient."

of the proposed project (*i.e.*, the active “ingredients” that are hypothesized to be critical to achieving the relevant outcomes) and describes the theoretical and operational relationships among the key project components and relevant outcomes.

Military- or veteran-connected student means one or more of the following:

(a) A child participating in an early learning program, a student enrolled in preschool through grade 12, or a student enrolled in career and technical education or postsecondary education who has a parent or guardian who is a member of the uniformed services (as defined by 37 U.S.C. 101), in the Army, Navy, Air Force, Marine Corps, Coast Guard, Space Force, National Guard, Reserves, National Oceanic and Atmospheric Administration, or Public Health Service or is a veteran of the uniformed services with an honorable discharge (as defined by 38 U.S.C. 3311).

(b) A student who is a member of the uniformed services, a veteran of the uniformed services, or the spouse of a service member or veteran.

(c) A child participating in an early learning program, a student enrolled in preschool through grade 12, or a student enrolled in career and technical education or postsecondary education who has a parent or guardian who is a veteran of the uniformed services (as defined by 37 U.S.C. 101).

Moderate evidence means that there is evidence of effectiveness of a key project component in improving a relevant outcome for a sample that overlaps with the populations or settings proposed to receive that component, based on a relevant finding from one of the following:

(1) A practice guide prepared by the WWC using version 2.1, 3.0, 4.0, or 4.1 of the WWC Handbooks reporting a “strong evidence base” or “moderate evidence base” for the corresponding practice guide recommendation;

(2) An intervention report prepared by the WWC using version 2.1, 3.0, 4.0, or 4.1 of the WWC Handbooks reporting a “positive effect” or “potentially positive effect” on a relevant outcome based on a “medium to large” extent of evidence, with no reporting of a “negative effect” or “potentially negative effect” on a relevant outcome; or

(3) A single experimental study or quasi-experimental design study reviewed and reported by the WWC using version 2.1, 3.0, 4.0, or 4.1 of the WWC Handbooks, or otherwise assessed by the Department using version 4.1 of the WWC Handbooks, as appropriate, and that—

(i) Meets WWC standards with or without reservations;

(ii) Includes at least one statistically significant and positive (*i.e.*, favorable) effect on a relevant outcome;

(iii) Includes no overriding statistically significant and negative effects on relevant outcomes reported in the study or in a corresponding WWC intervention report prepared under version 2.1, 3.0, 4.0, or 4.1 of the WWC Handbooks; and

(iv) Is based on a sample from more than one site (*e.g.*, State, county, city, school district, or postsecondary campus) and includes at least 350 students or other individuals across sites. Multiple studies of the same project component that each meet requirements in paragraphs (3)(i), (ii), and (iii) of this definition may together satisfy this requirement.

Parent includes a legal guardian or other person standing in loco parentis (such as a grandparent or stepparent with whom the child lives, or a person who is legally responsible for the child’s welfare).

Partner institution means an IHE, which may include a two-year IHE offering a dual program with a four-year IHE, participating in an eligible partnership that has a teacher preparation program—

(1) Whose graduates exhibit strong performance on State-determined qualifying assessments for new teachers through—

(i) Demonstrating that 80 percent or more of the graduates of the program who intend to enter the field of teaching have passed all of the applicable State qualification assessments for new teachers, which must include an assessment of each prospective teacher’s subject matter knowledge in the content area in which the teacher intends to teach; or

(ii) Being ranked among the highest performing teacher preparation programs in the State as determined by the State—

(A) Using criteria consistent with the requirements for the State report card under section 205(b) of the HEA (20 U.S.C. 1022d(b)) before the first publication of the report card; and

(B) Using the State report card on teacher preparation required under section 205(b) (20 U.S.C. 1022d(b)), after the first publication of such report card and for every year thereafter; and

(2) That requires—

(i) Each student in the program to meet high academic standards or demonstrate a record of success, as determined by the institution (including prior to entering and being accepted

into a program), and participate in intensive clinical experience;

(ii) Each student in the program preparing to become a teacher to meet the applicable State certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special education teachers, the qualifications described in section 612(a)(14)(C) of the IDEA (20 U.S.C. 1412(a)(14)(C)); and

(iii) Each student in the program preparing to become an early childhood educator to meet degree requirements, as established by the State, and become highly competent.

Principles of scientific research means principles of research that—

(1) Apply rigorous, systematic, and objective methodology to obtain reliable and valid knowledge relevant to education activities and programs;

(2) Present findings and make claims that are appropriate to, and supported by, the methods that have been employed; and

(3) Include, appropriate to the research being conducted—

(i) Use of systematic, empirical methods that draw on observation or experiment;

(ii) Use of data analyses that are adequate to support the general findings;

(iii) Reliance on measurements or observational methods that provide reliable and generalizable findings;

(iv) Strong claims of causal relationships, only with research designs that eliminate plausible competing explanations for observed results, such as, but not limited to, random-assignment experiments;

(v) Presentation of studies and methods in sufficient detail and clarity to allow for replication or, at a minimum, to offer the opportunity to build systematically on the findings of the research;

(vi) Acceptance by a peer-reviewed journal or critique by a panel of independent experts through a comparably rigorous, objective, and scientific review; and

(vii) Consistency of findings across multiple studies or sites to support the generality of results and conclusions.

Professional development means activities that—

(1) Are an integral part of school and LEA strategies for providing educators (including teachers, principals, other school leaders, specialized instructional support personnel, paraprofessionals, and, as applicable, early childhood educators) with the knowledge and skills necessary to enable students to succeed in a well-rounded education

and to meet the challenging State academic standards; and

(2) Are sustained (not stand-alone, one-day, or short term workshops), intensive, collaborative, job-embedded, data-driven, and classroom-focused, and may include activities that—

(i) Improve and increase teachers'—

(A) Knowledge of the academic subjects the teachers teach;

(B) Understanding of how students learn; and

(C) Ability to analyze student work and achievement from multiple sources, including how to adjust instructional strategies, assessments, and materials based on such analysis;

(ii) Are an integral part of broad schoolwide and districtwide educational improvement plans;

(iii) Allow personalized plans for each educator to address the educator's specific needs identified in observation or other feedback;

(iv) Improve classroom management skills;

(v) Support the recruitment, hiring, and training of effective teachers, including teachers who became certified through State and local alternative routes to certification; (vi) Advance teacher understanding of—

(A) Effective instructional strategies that are evidence-based; and

(B) Strategies for improving student academic achievement or substantially increasing the knowledge and teaching skills of teachers;

(vii) Are aligned with, and directly related to, academic goals of the school or LEA;

(viii) Are developed with extensive participation of teachers, principals, other school leaders, parents, representatives of Indian Tribes (as applicable), and administrators of schools to be served under the ESEA;

(ix) Are designed to give teachers of English learners, and other teachers and instructional staff, the knowledge and skills to provide instruction and appropriate language and academic support services to those children, including the appropriate use of curricula and assessments;

(x) To the extent appropriate, provide training for teachers, principals, and other school leaders in the use of technology (including education about the harms of copyright piracy), so that technology and technology applications are effectively used the classroom to improve teaching and learning in the curricula and academic subjects in which the teachers teach;

(xi) As a whole, are regularly evaluated for their impact on increased teacher effectiveness and improved student academic achievement, with the

findings of the evaluations used to improve the quality of professional development;

(xii) Are designed to give teachers of children with disabilities or children with developmental delays, and other teachers and instructional staff, the knowledge and skills to provide instruction and academic support services, to those children, including positive behavioral interventions and supports, multi-tier system of supports, and use of accommodations;

(xiii) Include instruction in the use of data and assessments to inform and instruct classroom practice;

(xiv) Include instruction in ways that teachers, principals, other school leaders, specialized instructional support personnel, and school administrators may work more effectively with parents and families;

(xv) Involve the forming of partnerships with IHEs, including, as applicable, Tribal Colleges and Universities as defined in section 316(b) of the HEA (20 U.S.C. 1059c(b)), to establish school-based teacher, principal, and other school leader training programs that provide prospective teachers, novice teachers, principals, and other school leaders with an opportunity to work under the guidance of experienced teachers, principals, other school leaders, and faculty of such institutions;

(xvi) Create programs to enable paraprofessionals (assisting teachers employed by an LEA receiving assistance under part A of title I of the ESEA) to obtain the education necessary for those paraprofessionals to become certified and licensed teachers;

(xvii) Provide follow-up training to teachers who have participated in activities described in this paragraph that are designed to ensure that the knowledge and skills learned by the teachers are implemented in the classroom; and

(xviii) Where practicable, provide jointly for school staff and other ECE program providers, to address the transition to elementary school, including issues related to school readiness.

Project component means an activity, strategy, intervention, process, product, practice, or policy included in a project. Evidence may pertain to an individual project component or to a combination of project components (e.g., training teachers on instructional practices for English learners and follow-on coaching for these teachers).

Promising evidence means that there is evidence of the effectiveness of a key project component in improving a

relevant outcome, based on a relevant finding from one of the following:

(1) A practice guide prepared by WWC reporting a “strong evidence base” or “moderate evidence base” for the corresponding practice guide recommendation;

(2) An intervention report prepared by the WWC reporting a “positive effect” or “potentially positive effect” on a relevant outcome with no reporting of a “negative effect” or “potentially negative effect” on a relevant outcome; or

(3) A single study assessed by the Department, as appropriate, that—

(i) Is an experimental study, a quasi-experimental design study, or a well-designed and well-implemented correlational study with statistical controls for selection bias (e.g., a study using regression methods to account for differences between a treatment group and a comparison group); and

(ii) Includes at least one statistically significant and positive (i.e., favorable) effect on a relevant outcome.

Quasi-experimental design study means a study using a design that attempts to approximate an experimental study by identifying a comparison group that is similar to the treatment group in important respects. This type of study, depending on design and implementation (e.g., establishment of baseline equivalence of the groups being compared), can meet WWC standards with reservations, but cannot meet WWC standards without reservations, as described in the WWC Handbooks.

Relevant outcome means the student outcome(s) or other outcome(s) the key project component is designed to improve, consistent with the specific goals of the program.

Scientifically valid research means applied research, basic research, and field-initiated research in which the rationale, design, and interpretation are soundly developed in accordance with principles of scientific research.

Strong evidence means that there is evidence of the effectiveness of a key project component in improving a relevant outcome for a sample that overlaps with the populations and settings proposed to receive that component, based on a relevant finding from one of the following:

(1) A practice guide prepared by the WWC using version 2.1, 3.0, 4.0, or 4.1 of the WWC Handbooks reporting a “strong evidence base” for the corresponding practice guide recommendation;

(2) An intervention report prepared by the WWC using version 2.1, 3.0, 4.0, or 4.1 of the WWC Handbooks reporting a

“positive effect” on a relevant outcome based on a “medium to large” extent of evidence, with no reporting of a “negative effect” or “potentially negative effect” on a relevant outcome; or

(3) A single experimental study reviewed and reported by the WWC using version 2.1, 3.0, 4.0, or 4.1 of the WWC Handbooks, or otherwise assessed by the Department using version 4.1 of the WWC Handbooks, as appropriate, and that—

(i) Meets WWC standards without reservations;

(ii) Includes at least one statistically significant and positive (*i.e.*, favorable) effect on a relevant outcome;

(iii) Includes no overriding statistically significant and negative effects on relevant outcomes reported in the study or in a corresponding WWC intervention report prepared under version 2.1, 3.0, 4.0, or 4.1 of the WWC Handbooks; and

(iv) Is based on a sample from more than one site (*e.g.*, State, county, city, school district, or postsecondary campus) and includes at least 350 students or other individuals across sites. Multiple studies of the same project component that each meet requirements in paragraphs (3)(i), (ii), and (iii) of this definition may together satisfy this requirement.

Teacher mentoring means the mentoring of new or prospective teachers through a program that—

(1) Includes clear criteria for the selection of teacher mentors who will provide role model relationships for mentees, which criteria must be developed by the eligible partnership and based on measures of teacher effectiveness;

(2) Provides high-quality training for such mentors, including instructional strategies for literacy instruction and classroom management (including approaches that improve the schoolwide climate for learning, which may include positive behavioral interventions and supports);

(3) Provides regular and ongoing opportunities for mentors and mentees to observe each other’s teaching methods in classroom settings during the day in a high-need school in the high-need LEA in the eligible partnership;

(4) Provides paid release time for mentors, as applicable;

(5) Provides mentoring to each mentee by a colleague who teaches in the same field, grade, or subject as the mentee;

(6) Promotes empirically-based practice of, and scientifically valid research on, where applicable—

(i) Teaching and learning;

(ii) Assessment of student learning;

(iii) The development of teaching skills through the use of instructional and behavioral interventions; and

(iv) The improvement of the mentees’ capacity to measurably advance student learning; and

(7) Includes—

(i) Common planning time or regularly scheduled collaboration for the mentor and mentee; and

(ii) Joint professional development opportunities.

Teaching residency program means a school-based teacher preparation program in which a prospective teacher—

(1) For one academic year, teaches alongside a mentor teacher, who is the teacher of record;

(2) Receives concurrent instruction during the year described in paragraph (1) from the partner institution, which courses may be taught by LEA personnel or residency program faculty, in the teaching of the content area in which the teacher will become certified or licensed;

(3) Acquires effective teaching skills; and

(4) Prior to completion of the program—

(i) Attains full State certification or licensure and, with respect to special education teachers, meets the qualifications described in section 612(a)(14)(C) of the IDEA (20 U.S.C. 1412(a)(14)(C)); and

(ii) Acquires a master’s degree not later than 18 months after beginning the program.

Teaching skills means skills that enable a teacher to—

(1) Increase student learning, achievement, and the ability to apply knowledge;

(2) Effectively convey and explain academic subject matter;

(3) Effectively teach higher-order analytical, evaluation, problem-solving, and communication skills;

(4) Employ strategies grounded in the disciplines of teaching and learning that—

(i) Are based on empirically-based practice and scientifically valid research, where applicable, related to teaching and learning;

(ii) Are specific to academic subject matter; and

(iii) Focus on the identification of students’ specific learning needs, particularly students with disabilities, students who are limited English proficient, students who are gifted and talented, and students with low literacy levels, and the tailoring of academic instruction to such needs;

(5) Conduct an ongoing assessment of student learning, which may include the

use of formative assessments, performance-based assessments, project-based assessments, or portfolio assessments, that measures higher-order thinking skills (including application, analysis, synthesis, and evaluation);

(6) Effectively manage a classroom, including the ability to implement positive behavioral interventions and support strategies;

(7) Communicate and work with parents, and involve parents in their children’s education; and

(8) Use, in the case of an early childhood educator, age-appropriate and developmentally appropriate strategies and practices for children in early childhood education programs.

Underserved student means a student (which may include children in early learning environments and students in K–12 programs) in one or more of the following subgroups:

(1) A student who is living in poverty or is served by schools with high concentrations of students living in poverty.

(2) A student of color.

(3) A student who is a member of a federally recognized Indian Tribe.

(4) An English learner.

(5) A child or student with a disability.

(6) A disconnected youth.

(7) A technologically unconnected youth.

(8) A migrant student.

(9) A student experiencing homelessness or housing insecurity.

(10) A lesbian, gay, bisexual, transgender, queer or questioning, or intersex (LGBTQI+) student.

(11) A student who is in foster care.

(12) A student without documentation of immigration status.

(13) A pregnant, parenting, or caregiving student.

(14) A student impacted by the justice system, including a formerly incarcerated student.

(15) A student who is the first in their family to attend postsecondary education.

(16) A student enrolling in or seeking to enroll in postsecondary education for the first time at the age of 20 or older.

(17) A student who is working full-time while enrolled in postsecondary education.

(18) A student who is enrolled in or is seeking to enroll in postsecondary education who is eligible for a Pell Grant.

(19) An adult student in need of improving their basic skills or an adult student with limited English proficiency.

(20) A student performing significantly below grade level.

(21) A military- or veteran-connected student.

For purposes of the definition of underserved student only—

Child or student with a disability means a child with disabilities as defined in section 602(3) of the Individuals with Disabilities Education Act (IDEA) (20 U.S.C. 1401(3)) and 34 CFR 300.8, or a student with disabilities, as defined in the Rehabilitation Act of 1973 (29 U.S.C. 705(37), 705(20)(B)); and

English learner means an individual who is an English learner as defined in section 8101(20) of the Elementary and Secondary Education Act of 1965, as amended, or an individual who is an English language learner as defined in section 203(7) of the Workforce Innovation and Opportunity Act.

What Works Clearinghouse (WWC) Handbooks (WWC Handbooks) means the standards and procedures set forth in the WWC Standards Handbook, Versions 4.0 or 4.1, and WWC Procedures Handbook, Versions 4.0 or 4.1, or in the WWC Procedures and Standards Handbook, Version 3.0 or Version 2.1 (all incorporated by reference, see § 77.2). Study findings eligible for review under WWC standards can meet WWC standards without reservations, meet WWC standards with reservations, or not meet WWC standards. WWC practice guides and intervention reports include findings from systematic reviews of evidence as described in the WWC Handbooks documentation.

Note: The What Works Clearinghouse Procedures and Standards Handbook (Version 4.1), as well as the more recent What Works Clearinghouse Handbooks released in August 2022 (Version 5.0), are available at <https://ies.ed.gov/ncee/wwc/Handbooks>.

Program Authority: 20 U.S.C. 1021–1022c.

Note: Projects will be awarded and must be operated in a manner consistent with the nondiscrimination requirements contained in Federal civil rights laws.

Applicable Regulations: (a) The Education Department General Administrative Regulations in 34 CFR parts 75, 77, 79, 82, 84, 86, 97, 98, and 99. (b) The Office of Management and Budget (OMB) Guidelines to Agencies on Governmentwide Debarment and Suspension (Nonprocurement) in 2 CFR part 180, as adopted and amended as regulations of the Department in 2 CFR part 3485. (c) The Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards in 2 CFR part 200, as adopted and amended as regulations of

the Department in 2 CFR part 3474 (Uniform Guidance). (d) The EED NFP. (e) The Supplemental Priorities.

Note: The regulations in 34 CFR part 86 apply to IHEs only.

II. Award Information

Type of Award: Discretionary grants.
Estimated Available Funds: \$25,000,000.

We intend to use an estimated \$25,000,000 for this FY 2024 competition.

Contingent upon the availability of funds and the quality of applications, we may make additional awards in subsequent years from the list of unfunded applications from this competition.

Estimated Range of Awards: \$500,000–\$2,000,000.

Estimated Average Size of Awards: \$1,000,000 for the first year of the project. Funding for the second, third, fourth, and fifth years is subject to the availability of funds and the approval of continuation awards (see 34 CFR 75.253).

Maximum Award: We will not make an award exceeding \$2,000,000 to any applicant per 12-month budget period.

Estimated Number of Awards: 15–17.

Note: The Department is not bound by any estimates in this notice.

Project Period: 60 months.

III. Eligibility Information

1. *Eligible Applicants:* An eligible applicant must be an “eligible partnership” as defined in section 200(6) of the HEA. The term “eligible partnership” means an entity that—

- (1) Must include—
 - (i) A high-need LEA;
 - (ii)(A) A high-need school or a consortium of high-need schools served by the high-need LEA; or
 - (B) As applicable, a high-need ECE program;
 - (iii) A partner institution;
 - (iv) A school, department, or program of education within such partner institution, which may include an existing teacher professional development program with proven outcomes within a four-year IHE that provides intensive and sustained collaboration between faculty and LEAs consistent with the requirements of title II of the HEA; and

(v) A school or department of arts and sciences within such partner institution; and

(2) May include any of the following:

- (i) The Governor of the State.
- (ii) The State educational agency (SEA).
- (iii) The State board of education.
- (iv) The State agency for higher education.

(v) A business.

(vi) A public or private nonprofit educational organization.

(vii) An educational service agency.

(viii) A teacher organization.

(ix) A high-performing LEA, or a consortium of such LEAs, that can serve as a resource to the partnership.

(x) A charter school.

(xi) A school or department within the partner institution that focuses on psychology and human development.

(xii) A school or department within the partner institution with comparable expertise in the disciplines of teaching, learning, and child and adolescent development.

(xiii) An entity operating a program that provides alternative routes to State certification of teachers.

Note: So that the Department can confirm the eligibility of the LEA(s) that an applicant proposes to serve, applicants must include information in their applications that demonstrates that each LEA to potentially be served by the project is a “high-need LEA” (as defined in this notice). Applicants should review the application package for additional information on determining whether an LEA meets the definition of “high-need LEA.”

Note: An LEA includes a public charter school that operates as an LEA.

Note: As required by HEA section 203(a)(2), an eligible partnership may not receive more than one grant during a five-year period. More information on eligible partnerships can be found in the TQP FAQ document on the program website at <https://oese.ed.gov/offices/office-of-discretionary-grants-support-services/effective-educator-development-programs/teacher-quality-partnership/applicant-info-and-eligibility/>.

2.a. *Cost Sharing or Matching:* Under section 203(c) of the HEA (20 U.S.C. 1022b(c)), each grant recipient must provide, from non-Federal sources, an amount equal to 100 percent of the amount of the grant, which may be provided in cash or in-kind, to carry out the activities supported by the grant. Applicants should budget their cost share or matching contributions on an annual basis for the entire five-year project period. Applicants must use the TQP Budget Worksheet to provide evidence of how they propose to meet their cost share or matching contributions for the entire five-year project period.

Consistent with 2 CFR 200.306(b) of the Uniform Guidance, any cost share or matching funds must be an allowable use of funds consistent with the cost principles detailed in Subpart E of the Uniform Guidance, and not included as

a contribution for any other Federal award. Section 203(c) of the HEA authorizes the Secretary to waive this cost share or matching requirement for any fiscal year for an eligible partnership if the Secretary determines that applying the cost share or matching requirement to the eligible partnership would result in serious hardship or an inability to carry out authorized TQP program activities. The Secretary does not, as a general matter, anticipate waiving this requirement in the future. Furthermore, given the importance of cost share or matching funds to the long-term success of the project, eligible entities must identify appropriate cost share or matching funds for the proposed five-year project period. Finally, the selection criteria include factors such as “the adequacy of support, including facilities, equipment, supplies, and other resources, from the applicant organization or the lead applicant organization” and “the extent to which the applicant demonstrates that it has the resources to operate the project beyond the length of the grant, including a multi-year financial and operating model and accompanying plan; the demonstrated commitment of any partners; evidence of broad support from stakeholders (e.g., SEAs, teachers’ unions) critical to the project’s long term success; or more than one of these types of evidence” which may include a consideration of demonstrated cost share or matching support.

Note: The combination of Federal and non-Federal funds should equal the total cost of the project. Therefore, grantees are required to support no less than 50 percent of the total cost of the project with non-Federal funds. Grantees are strongly encouraged to take this requirement into account when requesting Federal funds. Grantees must budget their requests accordingly and must verify that their budgets reflect the cost allocations appropriately. (Cost Share or Matching Formula: Total Project Cost divided by two equals Federal Award Amount).

b. *Supplement-Not-Supplant:* This program involves supplement-not-supplant funding requirements. In accordance with section 202(k) of the HEA (20 U.S.C. 1022a(k)), funds made available under this program must be used to supplement, and not supplant, other Federal, State, and local funds that would otherwise be expended to carry out activities under this program. Additionally, the supplement-not-supplant requirement applies to all cost share or matching funds under the program.

c. *Indirect Cost Rate Information:* This program uses a training indirect cost

rate. This limits indirect cost reimbursement to an entity’s actual indirect costs, as determined in its negotiated indirect cost rate agreement, or eight percent of a modified total direct cost base, whichever amount is less. For more information regarding training indirect cost rates, see 34 CFR 75.562. For more information regarding indirect costs, or to obtain a negotiated indirect cost rate, please see <https://www2.ed.gov/about/offices/list/ocfo/intro.html>.

3. *Subgrantees:* Under 34 CFR 75.708(b) and (c), a grantee under this competition may award subgrants to directly carry out project activities described in its application to the following types of entities: LEAs, SEAs, nonprofit organizations, or a business. The grantee may award subgrants to entities it has identified in an approved application.

4.a. *Limitation on Administrative Expenses:* Under HEA section 203(d) (20 U.S.C. 1022b(d)), an eligible partnership that receives a grant under this program may not use more than two percent of the funds provided to administer the grant.

b. *General Application Requirements:* All applicants must meet the following general application requirements in order to be considered for funding. The general application requirements are from HEA section 202(b) (20 U.S.C. 1022a(b)). Each eligible partnership desiring a grant under this program must submit an application that contains—

(a) A needs assessment of the partners in the eligible partnership with respect to the preparation, ongoing training, professional development, and retention of general education and special education teachers, principals, and, as applicable, early childhood educators;

(b) A description of the extent to which the program to be carried out with grant funds, as described in the applicable absolute priority, will prepare prospective and new teachers with strong teaching skills;

(c) A description of how such a program will prepare prospective and new teachers to understand and use research and data to modify and improve classroom instruction;

(d) A description of—

(1) How the eligible partnership will coordinate strategies and activities assisted under the grant with other teacher preparation or professional development programs, including programs funded under the ESEA and the IDEA, and through the National Science Foundation; and

(2) How the activities of the partnership will be consistent with

State, local, and other education reform activities that promote teacher quality and student academic achievement;

(e) An assessment that describes the resources available to the eligible partnership, including—

(1) The integration of funds from other related sources;

(2) The intended use of the grant funds; and

(3) The commitment of the resources of the partnership to the activities assisted under this program, including financial support, faculty participation, and time commitments, and to the continuation of the activities when the grant ends;

(f) A description of—

(1) How the eligible partnership will meet the purposes of the TQP program as specified in section 201 of the HEA;

(2) How the partnership will carry out the activities required under the applicable absolute priority, based on the needs identified in paragraph (a), with the goal of improving student academic achievement;

(3) If the partnership chooses to use funds under this section for a project or activities under section 202(f) of the HEA, how the partnership will carry out such project or required activities based on the needs identified in paragraph (a), with the goal of improving student academic achievement;

(4) The partnership’s evaluation plan under section 204(a) of the HEA;

(5) How the partnership will align the teacher preparation program with the—

(i) State early learning standards for ECE programs, as appropriate, and with the relevant domains of early childhood development; and

(ii) Challenging State academic standards under section 1111(b)(1) of the ESEA, established by the State in which the partnership is located;

(6) How the partnership will prepare general education teachers to teach students with disabilities, including training related to participation as a member of individualized education program teams, as defined in section 614(d)(1)(B) of the IDEA;

(7) How the partnership will prepare general education and special education teachers to teach students who are limited English proficient;

(8) How faculty at the partner institution will work during the term of the grant, with teachers who meet the applicable State certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special education teachers, the qualifications described in section 612(a)(14)(C) of the IDEA, in the classrooms of high-need

schools served by the high-need LEA in the partnership to—

(i) Provide high-quality professional development activities to strengthen the content knowledge and teaching skills of elementary school and secondary school teachers; and

(ii) Train other classroom teachers to implement literacy programs that incorporate the essential components of reading instruction;

(9) How the partnership will design, implement, or enhance a year-long and rigorous teaching preservice clinical program component;

(10) How the partnership will support in-service professional development strategies and activities; and

(11) How the partnership will collect, analyze, and use data on the retention of all teachers and early childhood educators in schools and ECE programs located in the geographic area served by the partnership to evaluate the effectiveness of the partnership's teacher and educator support system; and

(g) With respect to the induction program required as part of the activities carried out under the applicable absolute priority—

(1) A demonstration that the schools and departments within the IHE that are part of the induction program will effectively prepare teachers, including providing content expertise and expertise in teaching, as appropriate;

(2) A demonstration of the eligible partnership's capability and commitment to, and the accessibility to and involvement of faculty in, the use of empirically-based practice and scientifically valid research on teaching and learning;

(3) A description of how the teacher preparation program will design and implement an induction program to support, through not less than the first two years of teaching, all new teachers who are prepared by the teacher preparation program in the partnership and who teach in the high-need LEA in the partnership, and, to the extent practicable, all new teachers who teach in such high-need LEA, in the further development of the new teachers' teaching skills, including the use of mentors who are trained and compensated by such program for the mentors' work with new teachers; and

(4) A description of how faculty involved in the induction program will be able to substantially participate in an ECE program or elementary school or secondary school classroom setting, as applicable, including release time and receiving workload credit for such participation.

IV. Application and Submission Information

1. Application Submission

Instructions: Applicants are required to follow the Common Instructions for Applicants to Department of Education Discretionary Grant Programs, published in the **Federal Register** on December 7, 2022 (87 FR 75045) and available at www.federalregister.gov/documents/2022/12/07/2022-26554/common-instructions-for-applicants-to-department-of-education-discretionary-grant-programs, which contain requirements and information on how to submit an application.

2. Submission of Proprietary

Information: Given the types of projects that may be proposed in applications for the TQP program, your application may include business information that you consider proprietary. In 34 CFR 5.11, we define "business information" and describe the process we use in determining whether any of that information is proprietary and, thus, protected from disclosure under Exemption 4 of the Freedom of Information Act (5 U.S.C. 552, as amended).

Because we plan to make successful applications available to the public, you may wish to request confidentiality of business information.

Consistent with Executive Order 12600 (Predisclosure Notification Procedures for Confidential Commercial Information), please designate in your application any information that you believe is exempt from disclosure under Exemption 4. In the appropriate Appendix section of your application, under "Other Attachments Form," please list the page number or numbers on which we can find this information. For additional information please see 34 CFR 5.11(c).

3. *Intergovernmental Review:* This program is subject to Executive Order 12372 and the regulations in 34 CFR part 79. Information about Intergovernmental Review of Federal Programs under Executive Order 12372 is in the application package for this competition.

4. *Funding Restrictions:* We specify unallowable costs in 2 CFR 200, subpart E. We reference additional regulations outlining funding restrictions in the *Applicable Regulations* section of this notice.

Note: Tuition is not an allowable use of funds under this program.

5. *Recommended Page Limit:* The application narrative is where you, the applicant, address the selection criteria that reviewers use to evaluate your application. We recommend that you (1)

limit the application narrative to no more than 50 pages and (2) use the following standards:

A "page" is 8.5" x 11", on one side only, with 1" margins at the top, bottom, and both sides.

- Double space (no more than three lines per vertical inch) all text in the application narrative, including titles, headings, footnotes, quotations, references, and captions, as well as all text in charts, tables, figures, and graphs.

- Use a font that is either 12 point or larger or no smaller than 10 pitch (characters per inch).

- Use one of the following fonts: Times New Roman, Courier, Courier New, or Arial.

Furthermore, applicants are strongly encouraged to include a table of contents that specifies where each required part of the application is located.

6. *Notice of Intent to Apply:* The Department will be able to develop a more efficient process for reviewing grant applications if it has a better understanding of the number of entities that intend to apply for funding under this competition. Therefore, the Secretary strongly encourages each potential applicant to notify the Department of its intent to submit an application for funding by sending an email to TQPPartnership@ed.gov, by the date listed in the **DATES** section at the beginning of this notice, with FY 2024 TQP Intent to Apply in the subject line. Applicants that do not send a notice of intent to apply may still apply for funding.

V. Application Review Information

1. *Selection Criteria:* The selection criteria for this competition are from 34 CFR 75.210. An applicant may earn up to a total of 100 points based on the selection criteria. The maximum score for each criterion is indicated in parentheses. Each criterion also includes the factors that the reviewers will consider in determining how well an application meets the criterion.

The criteria are as follows:

(a) *Quality of the project design* (up to 30 points).

The Secretary considers the quality of the design of the proposed project. In determining the quality of the design of the proposed project, the Secretary considers the following factors:

(i) The extent to which the proposed project demonstrates a rationale.

(ii) The extent to which the goals, objectives, and outcomes to be achieved by the proposed project are clearly specified and measurable.

(iii) The extent to which the proposed project is part of a comprehensive effort to improve teaching and learning and support rigorous academic standards for students.

(iv) The extent to which the design of the proposed project reflects up-to-date knowledge from research and effective practice.

(v) The extent to which performance feedback and continuous improvement are integral to the design of the proposed project.

(vi) The extent to which the proposed project is designed to build capacity and yield results that will extend beyond the period of Federal financial assistance.

(b) *Quality of the project evaluation* (up to 20 points).

The Secretary considers the quality of the evaluation to be conducted of the proposed project. In determining the quality of the evaluation, the Secretary considers the following factors:

(i) The extent to which the methods of evaluation will provide valid and reliable performance data on relevant outcomes.

(ii) The extent to which the methods of evaluation are thorough, feasible, and appropriate to the goals, objectives, and outcomes of the proposed project.

(c) *Adequacy of resources* (up to 30 points).

The Secretary considers the adequacy of resources for the proposed project. In determining the adequacy of resources for the proposed project, the Secretary considers the following factors:

(i) The adequacy of support, including facilities, equipment, supplies, and other resources, from the applicant organization or the lead applicant organization.

(ii) The extent to which the budget is adequate to support the proposed project.

(iii) The extent to which the costs are reasonable in relation to the objectives, design, and potential significance of the proposed project.

(iv) The extent to which the applicant demonstrates that it has the resources to operate the project beyond the length of the grant, including a multi-year financial and operating model and accompanying plan; the demonstrated commitment of any partners; evidence of broad support from stakeholders (e.g., SEAs, teachers' unions) critical to the project's long-term success; or more than one of these types of evidence.

(v) The relevance and demonstrated commitment of each partner in the proposed project to the implementation and success of the project.

(d) *Quality of the management plan* (up to 20 points).

The Secretary considers the quality of the management plan for the proposed

project. In determining the quality of the management plan for the proposed project, the Secretary considers the following factors:

(i) The adequacy of the management plan to achieve the objectives of the proposed project on time and within budget, including clearly defined responsibilities, timelines, and milestones for accomplishing project tasks.

(ii) The adequacy of procedures for ensuring feedback and continuous improvement in the operation of the proposed project.

2. *Review and Selection Process:* We remind potential applicants that in reviewing applications in any discretionary grant competition, the Secretary may consider, under 34 CFR 75.217(d)(3), the past performance of the applicant in carrying out a previous award, such as the applicant's use of funds, achievement of project objectives, and compliance with grant conditions. The Secretary may also consider whether the applicant failed to submit a timely performance report or submitted a report of unacceptable quality. In addition, in making a competitive grant award, the Secretary requires various assurances, including those applicable to Federal civil rights laws that prohibit discrimination in programs or activities receiving Federal financial assistance from the Department (34 CFR 100.4, 104.5, 106.4, 108.8, and 110.23).

3. *Risk Assessment and Specific Conditions:* Consistent with 2 CFR 200.206, before awarding grants under this competition the Department conducts a review of the risks posed by applicants. Under 2 CFR 200.208, the Secretary may impose specific conditions and, under 2 CFR 3474.10, in appropriate circumstances, high-risk conditions on a grant if the applicant or grantee is not financially stable; has a history of unsatisfactory performance; has a financial or other management system that does not meet the standards in 2 CFR part 200, subpart D; has not fulfilled the conditions of a prior grant; or is otherwise not responsible.

4. *Integrity and Performance System:* If you are selected under this competition to receive an award that over the course of the project period may exceed the simplified acquisition threshold (currently \$250,000), we must make a judgment about your integrity, business ethics, and record of performance under Federal awards—that is, the risk posed by you as an applicant—before we make an award. In doing so, we must consider any information about you that is in the integrity and performance system

(currently referred to as the Federal Awardee Performance and Integrity Information System (FAPIIS)), accessible through the System for Award Management. You may review and comment on any information about yourself that a Federal agency previously entered and that is currently in FAPIIS. Please note that, if the total value of your currently active grants, cooperative agreements, and procurement contracts from the Federal Government exceeds \$10,000,000, the reporting requirements in 2 CFR part 200, Appendix XII, require you to report certain integrity information to FAPIIS semiannually. Please review the requirements in 2 CFR part 200, Appendix XII, if this grant plus all the other Federal funds you receive exceed \$10,000,000.

5. *In General:* In accordance with the Uniform Guidance located at 2 CFR part 200, all applicable Federal laws, and relevant Executive guidance, the Department will review and consider applications for funding pursuant to this notice inviting applications in accordance with—

(a) Selecting recipients most likely to be successful in delivering results based on the program objectives through an objective process of evaluating Federal award applications (2 CFR 200.205);

(b) Prohibiting the purchase of certain telecommunication and video surveillance services or equipment in alignment with section 889 of the National Defense Authorization Act of 2019 (Pub. L. 115–232) (2 CFR 200.216);

(c) Providing a preference, to the extent permitted by law, to maximize use of goods, products, and materials produced in the United States (2 CFR 200.322); and

(d) Terminating agreements in whole or in part to the greatest extent authorized by law if an award no longer effectuates the program goals or agency priorities (2 CFR 200.340).

VI. Award Administration Information

1. *Award Notices:* If your application is successful, we notify your U.S. Representative and U.S. Senators and send you a Grant Award Notification (GAN); or we may send you an email containing a link to access an electronic version of your GAN. We may notify you informally, also. If your application is not evaluated or not selected for funding, we notify you.

2. *Administrative and National Policy Requirements:* We identify administrative and national policy requirements in the application package and reference these and other requirements in the *Applicable Regulations* section of this notice. We

reference the regulations outlining the terms and conditions of an award in the *Applicable Regulations* section of this notice and include these and other specific conditions in the GAN. The GAN also incorporates your approved application as part of your binding commitments under the grant.

3. *Open Licensing Requirements:* Unless an exception applies, if you are awarded a grant under this competition, you will be required to openly license to the public grant deliverables created in whole, or in part, with Department grant funds. When the deliverable consists of modifications to pre-existing works, the license extends only to those modifications that can be separately identified and only to the extent that open licensing is permitted under the terms of any licenses or other legal restrictions on the use of pre-existing works. Additionally, a grantee or subgrantee that is awarded competitive grant funds must have a plan to disseminate these public grant deliverables. This dissemination plan can be developed and submitted after your application has been reviewed and selected for funding. For additional information on the open licensing requirements please refer to 2 CFR 3474.20.

4. *Reporting:* (a) If you apply for a grant under this competition, you must ensure that you have in place the necessary processes and systems to comply with the reporting requirements in 2 CFR part 170 should you receive funding under the competition. This does not apply if you have an exception under 2 CFR 170.110(b).

(b) At the end of your project period, you must submit a final performance report, including financial information, as directed by the Secretary. If you receive a multiyear award, you must submit an annual performance report that provides the most current performance and financial expenditure information as directed by the Secretary under 34 CFR 75.118. The Secretary may also require more frequent performance reports under 34 CFR 75.720(c). For specific requirements on reporting, please go to www.ed.gov/fund/grant/apply/appforms/appforms.html.

(c) Under 34 CFR 75.250(b), the Secretary may provide a grantee with additional funding for data collection analysis and reporting. In this case the Secretary establishes a data collection period.

5. *Performance Measures:* For purposes of Department reporting under 34 CFR 75.110, the following measures will be used by the Department to evaluate the overall effectiveness of the

grantee's project, as well as the TQP program as a whole:

(a) Performance Measure 1: Certification/Licensure. The percentage of program graduates who have attained initial State certification/licensure by passing all necessary licensure/certification assessments within one year of program completion.

(b) Performance Measure 2: Shortage Area Certification. The percentage of participating teachers fully certified in teaching math/science, special education, students who are limited English proficient, and other identified teacher shortage areas where program graduates that attain initial certification/licensure by passing all necessary licensure/certification assessments within one year of program completion, if applicable to the applicant or grantee's project.

(c) Performance Measure 3: One-Year Persistence. The percentage of program participants who were enrolled in the postsecondary program in the previous grant reporting period who did not graduate and persisted in the postsecondary program in the current grant reporting period.

(d) Performance Measure 4: One-Year Employment Retention. The percentage of program completers who were employed for the first time as teachers of record in the preceding year by the partner high-need LEA or ECE program and were retained for the current school year.

(e) Performance Measure 5: Three-Year Employment Retention. The percentage of program completers who were employed by the partner high-need LEA or ECE program for three consecutive years after initial employment.

(f) Efficiency Measure: The Federal cost per program completer. (These data will not be available until the final year of the project period.)

Note: If funded, grantees will be asked to collect and report data on these measures in their project's annual performance reports (34 CFR 75.590). Applicants are also advised to consider these measures in conceptualizing the design, implementation, and evaluation of their proposed projects because of their importance in the application review process. Collection of data on these measures should be a part of the evaluation plan, along with measures of progress on goals and objectives that are specific to your project.

All grantees will be expected to submit an annual performance report documenting their success in addressing these performance measures.

Applicants must also address the evaluation requirements in section

204(a) of the HEA (20 U.S.C. 1022c(a)). This section asks applicants to develop objectives and measures for increasing—

(1) Achievement for all prospective and new teachers, as measured by the eligible partnership;

(2) Teacher retention in the first three years of a teacher's career;

(3) Improvement in the pass rates and scaled scores for initial State certification or licensure of teachers; and

(4) The percentage of teachers who meet the applicable State certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special education teachers, the qualifications described in section 612(a)(14)(C) of the IDEA (20 U.S.C. 1412(a)(14)(C)), hired by the high-need LEA participating in the eligible partnership;

(5) The percentage of teachers who meet the applicable State certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special education teachers, the qualifications described in section 612(a)(14)(C) of the IDEA (20 U.S.C. 1412(a)(14)(C)), hired by the high-need LEA who are members of underrepresented groups;

(6) The percentage of teachers who meet the applicable State certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special education teachers, the qualifications described in section 612(a)(14)(C) of the IDEA (20 U.S.C. 1412(a)(14)(C)), hired by the high-need LEA who teach high-need academic subject areas (such as reading, mathematics, science, and foreign language, including less commonly taught languages and critical foreign languages);

(7) The percentage of teachers who meet the applicable State certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special education teachers, the qualifications described in section 612(a)(14)(C) of the IDEA (20 U.S.C. 1412(a)(14)(C)), hired by the high-need LEA who teach in high-need areas (including special education, language instruction educational programs for limited English proficient students, and ECE);

(8) The percentage of teachers who meet the applicable State certification and licensure requirements, including any requirements for certification obtained through alternative routes to certification, or, with regard to special

education teachers, the qualifications described in section 612(a)(14)(C) of the IDEA (20 U.S.C. 1412(a)(14)(C)), hired by the high-need LEA who teach in high-need schools, disaggregated by the elementary school and secondary school levels;

(9) As applicable, the percentage of ECE program classes in the geographic area served by the eligible partnership taught by early childhood educators who are highly competent; and

(10) As applicable, the percentage of teachers trained—

(i) To integrate technology effectively into curricula and instruction, including technology consistent with the principles of universal design for learning; and

(ii) To use technology effectively to collect, manage, and analyze data to improve teaching and learning for the purpose of improving student academic achievement.

6. *Continuation Awards:* In making a continuation award under 34 CFR 75.253, the Secretary considers, among other things: whether a grantee has made substantial progress in achieving the goals and objectives of the project; whether the grantee has expended funds in a manner that is consistent with its approved application and budget; whether the grantee has met the required non-Federal cost share or matching requirement; and, if the Secretary has established performance measurement requirements, whether the grantee has made substantial progress in achieving the performance targets in the grantee's approved application.

In making a continuation award, the Secretary also considers whether the grantee is operating in compliance with the assurances in its approved application, including those applicable to Federal civil rights laws that prohibit discrimination in programs or activities receiving Federal financial assistance from the Department (34 CFR 100.4, 104.5, 106.4, 108.8, and 110.23).

VII. Other Information

Accessible Format: On request to the program contact person listed under **FOR FURTHER INFORMATION CONTACT**, individuals with disabilities can obtain this document and a copy of the application package in an accessible format. The Department will provide the requestor with an accessible format that may include Rich Text Format (RTF) or text format (txt), a thumb drive, an MP3 file, braille, large print, audiotape, or compact disc, or other accessible format.

Electronic Access to This Document: The official version of this document is the document published in the **Federal Register**. You may access the official

edition of the **Federal Register** and the Code of Federal Regulations at <https://www.govinfo.gov>. At this site you can view this document, as well as all other documents of this Department published in the **Federal Register**, in text or Portable Document Format (PDF). To use PDF you must have Adobe Acrobat Reader, which is available free at the site. You may also access documents of the Department published in the **Federal Register** by using the article search feature at <https://www.federalregister.gov>. Specifically, through the advanced search feature at this site, you can limit your search to documents published by the Department.

Adam Schott,

Principal Deputy Assistant Secretary, Delegated the Authority to Perform the Functions and Duties of the Assistant Secretary for Elementary and Secondary Education.

[FR Doc. 2024-07183 Filed 4-3-24; 8:45 am]

BILLING CODE 4000-01-P

DEPARTMENT OF EDUCATION

[Docket No.: ED-2024-SCC-0015]

Agency Information Collection Activities; Submission to the Office of Management and Budget for Review and Approval; Comment Request; U.S. Department of Education Build America, Buy America Act (BABAA) Data Collection

AGENCY: Office of Finance and Operations (OFO), Department of Education (ED).

ACTION: Notice.

SUMMARY: In accordance with the Paperwork Reduction Act (PRA) of 1995, the Department is proposing a new information collection request (ICR).

DATES: Interested persons are invited to submit comments on or before May 6, 2024.

ADDRESSES: Written comments and recommendations for proposed information collection requests should be submitted within 30 days of publication of this notice. Click on this link www.reginfo.gov/public/do/PRAMain to access the site. Find this information collection request (ICR) by selecting "Department of Education" under "Currently Under Review," then check the "Only Show ICR for Public Comment" checkbox. *Reginfo.gov* provides two links to view documents related to this information collection request. Information collection forms and instructions may be found by

clicking on the "View Information Collection (IC) List" link. Supporting statements and other supporting documentation may be found by clicking on the "View Supporting Statement and Other Documents" link.

FOR FURTHER INFORMATION CONTACT: For specific questions related to collection activities, please contact Cleveland Knight, 202-987-0064.

SUPPLEMENTARY INFORMATION: The Department is especially interested in public comment addressing the following issues: (1) is this collection necessary to the proper functions of the Department; (2) will this information be processed and used in a timely manner; (3) is the estimate of burden accurate; (4) how might the Department enhance the quality, utility, and clarity of the information to be collected; and (5) how might the Department minimize the burden of this collection on the respondents, including through the use of information technology. Please note that written comments received in response to this notice will be considered public records.

Title of Collection: U.S. Department of Education Build America, Buy America Act (BABAA) Data Collection.

OMB Control Number: 1894-NEW.

Type of Review: A new ICR.

Respondents/Affected Public: State, Local, and Tribal Governments, Private Sector—Not-for-Profit Institutions.

Total Estimated Number of Annual Responses: 470.

Total Estimated Number of Annual Burden Hours: 4,700.

Abstract: In accordance with section 70914 of the Build America Buy America Act (Pub. L. 117-58 70901-70953) (BABAA), grantees funded under Department of Education (the Department) programs that allow funds to be used for infrastructure projects (infrastructure programs), *i.e.*, construction and broadband infrastructure, may not use their grant funds for these infrastructure projects or activities unless they comply with the following BABAA sourcing requirements:

1. All iron and steel used in the infrastructure project or activity are produced in the United States.
2. All manufactured products used in the infrastructure project or activity are produced in the United States.
3. All construction materials are manufactured in the United States.

The Department may, in accordance with sections 70914(b) and (d), 70921(b), 70935, and 70937 of BABAA, and the Office of Management and Budget Memorandum M 24-02, Implementation Guidance on

Application of Buy America Preference in Federal Financial Assistance Programs for Infrastructure, approve waivers to BABAA sourcing requirements under programs it has identified as infrastructure programs when it determines that exceptions to these requirements apply. The Department may approve these waivers, subject to notice and comment requirements and the Office of Management and Budget Made in America Office (MIAO) review.

The information submitted by grantees using the BABAA Data Collection Form will be used by the Department to track the type of waivers (*i.e.*, agency level waivers or approved grantee waivers) implemented by grantees. The data may also be used for reporting purposes.

Dated: April 1, 2024.

Stephanie Valentine,

PRA Coordinator, Strategic Collections and Clearance Governance and Strategy Division, Office of Chief Data Officer, Office of Planning, Evaluation and Policy Development.

[FR Doc. 2024-07166 Filed 4-3-24; 8:45 am]

BILLING CODE 4000-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

Combined Notice of Filings #1

Take notice that the Commission received the following exempt wholesale generator filings:

Docket Numbers: EG24-155-000.

Applicants: Cedar Springs Wind IV, LLC.

Description: Cedar Springs Wind IV, LLC submits Notice of Self-Certification of Exempt Wholesale Generator Status.

Filed Date: 3/29/24.

Accession Number: 20240329-5311.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: EG24-156-000.

Applicants: Anticline Wind, LLC.

Description: Anticline Wind, LLC submits Notice of Self-Certification of Exempt Wholesale Generator Status.

Filed Date: 3/29/24.

Accession Number: 20240329-5316.

Comment Date: 5 p.m. ET 4/19/24.

Take notice that the Commission received the following electric rate filings:

Docket Numbers: ER10-1586-010; ER10-1630-010.

Applicants: Wolf Hills Energy, LLC, Big Sandy Peaker Plant, LLC.

Description: Response to March 1, 2024 Deficiency Letter of Big Sandy Peaker Plant, LLC.

Filed Date: 3/28/24.

Accession Number: 20240328-5352.

Comment Date: 5 p.m. ET 4/18/24.

Docket Numbers: ER23-2359-006.

Applicants: PJM Interconnection, L.L.C.

Description: Tariff Amendment: Amendment to ISA/CSA SA Nos. 6967 & 6968; AD2-100/131—Docket ER23-2359 to be effective 9/6/2023.

Filed Date: 3/29/24.

Accession Number: 20240329-5117.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24-1270-000.

Applicants: Prescott Wind Energy LLC.

Description: Supplement to February 16, 2024 Prescott Wind Energy LLC tariff filing.

Filed Date: 3/27/24.

Accession Number: 20240327-5316.

Comment Date: 5 p.m. ET 4/10/24.

Docket Numbers: ER24-1638-000.

Applicants: Midcontinent Independent System Operator, Inc.

Description: 205(d) Rate Filing: 2024-03-28 Resource Accreditation Reform to be effective 9/1/2024.

Filed Date: 3/28/24.

Accession Number: 20240328-5329.

Comment Date: 5 p.m. ET 4/29/24.

Docket Numbers: ER24-1639-000.

Applicants: ITC Midwest LLC.

Description: 205(d) Rate Filing: Amended and Restated Joint Use Pole Agreement with Corn Belt (RS I90) to be effective 5/28/2024.

Filed Date: 3/28/24.

Accession Number: 20240328-5338.

Comment Date: 5 p.m. ET 4/18/24.

Docket Numbers: ER24-1640-000.

Applicants: Public Service Company of New Mexico.

Description: Annual Filing of Post-Employment Benefits Other than Pensions for 2024 of Public Service Company of New Mexico.

Filed Date: 3/28/24.

Accession Number: 20240328-5345.

Comment Date: 5 p.m. ET 4/18/24.

Docket Numbers: ER24-1641-000.

Applicants: Fuse Energy NY LLC.

Description: Baseline eTariff Filing: Application for Market Based Rate Authority to be effective 5/27/2024.

Filed Date: 3/28/24.

Accession Number: 20240328-5344.

Comment Date: 5 p.m. ET 4/18/24.

Docket Numbers: ER24-1642-000.

Applicants: Hecate Grid Swiftsure, LLC.

Description: Hecate Grid Swiftsure, LLC requests a one-time limited waiver of the New York Independent System Operator, Inc.'s Open Access Transmission Tariff to allow Hecate to extend the proposed commercial operation date.

Filed Date: 3/28/24.

Accession Number: 20240328-5381.

Comment Date: 5 p.m. ET 4/18/24.

Docket Numbers: ER24-1643-000.

Applicants: American Transmission Systems, Incorporated, PJM Interconnection, L.L.C.

Description: 205(d) Rate Filing: American Transmission Systems, Incorporated submits tariff filing per 35.13(a)(2)(iii): ATSI, Inc. submits OHTCo & ATSI IA SA No. 6936 to be effective 5/29/2024.

Filed Date: 3/29/24.

Accession Number: 20240329-5070.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24-1644-000.

Applicants: New York Independent System Operator, Inc., Niagara Mohawk Power Corporation.

Description: 205(d) Rate Filing: New York Independent System Operator, Inc. submits tariff filing per 35.13(a)(2)(iii): NYISO-NMPC Joint 205: Amnd LGIA for East Point Solar SA2683 to be effective 3/15/2024.

Filed Date: 3/29/24.

Accession Number: 20240329-5095.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24-1645-000.

Applicants: Idaho Power Company.

Description: 205(d) Rate Filing: SA #414—NITSA Between Idaho Power Company and PacifiCorp to be effective 6/1/2024.

Filed Date: 3/29/24.

Accession Number: 20240329-5101.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24-1646-000.

Applicants: Mississippi Power Company.

Description: Tariff Amendment: Notice of Termination of Gulf States TFA to be effective 5/31/2024.

Filed Date: 3/29/24.

Accession Number: 20240329-5105.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24-1647-000.

Applicants: PJM Interconnection, L.L.C.

Description: 205(d) Rate Filing: Amendment to ISA, SA No. 6667; Queue No. AE1-157 (amend) to be effective 5/29/2024.

Filed Date: 3/29/24.

Accession Number: 20240329-5107.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24-1648-000.

Applicants: Louisville Gas and Electric Company.

Description: 205(d) Rate Filing: Mill Creek 5 Provisional Large Generator Interconnection Agreement to be effective 3/7/2024.

Filed Date: 3/29/24.

Accession Number: 20240329-5139.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24–1649–000.
Applicants: PECO Energy Company, PJM Interconnection, L.L.C.

Description: 205(d) Rate Filing: PECO Energy Company submits tariff filing per 35.13(a)(2)(iii); PECO submits revisions to OATT Att. H–7A Depreciation Rates to be effective 5/29/2024.

Filed Date: 3/29/24.

Accession Number: 20240329–5158.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24–1650–000.

Applicants: New England Power Pool Participants Committee.

Description: 205(d) Rate Filing: Apr 2024 Membership Filing to be effective 3/1/2024.

Filed Date: 3/29/24.

Accession Number: 20240329–5194.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24–1651–000.

Applicants: Renew Home VPP, LLC.

Description: Baseline eTariff Filing: Baseline new to be effective 3/30/2024.

Filed Date: 3/29/24.

Accession Number: 20240329–5230.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24–1652–000.

Applicants: Mississippi Power Company.

Description: 205(d) Rate Filing: MRA 31 Rate Case Filing to be effective 5/29/2024.

Filed Date: 3/29/24.

Accession Number: 20240329–5248.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24–1653–000.

Applicants: MRP Pacifica Marketing LLC.

Description: Baseline eTariff Filing: Baseline new to be effective 5/29/2024.

Filed Date: 3/29/24.

Accession Number: 20240329–5270.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24–1654–000.

Applicants: Georgia Power Company.

Description: Initial rate filing: SR

Metter Affected System Construction Agreement Filing to be effective 6/22/2023.

Filed Date: 3/29/24.

Accession Number: 20240329–5273.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24–1655–000.

Applicants: New York Independent System Operator, Inc.

Description: 205(d) Rate Filing: NYISO 205: Financial Transaction Capabilities and Fast-Start Resource Scheduling to be effective 6/11/2024.

Filed Date: 3/29/24.

Accession Number: 20240329–5288.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24–1656–000.

Applicants: Furry Creek Power Ltd.

Description: Baseline eTariff Filing: Furry Creek Power Ltd. MBR Tariff to be effective 5/29/2024.

Filed Date: 3/29/24.

Accession Number: 20240329–5307.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24–1657–000.

Applicants: McNair Creek Hydro Limited Partnership.

Description: Baseline eTariff Filing: McNair Creek Hydro Limited Partnership MBR Tariff to be effective 5/29/2024.

Filed Date: 3/29/24.

Accession Number: 20240329–5309.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24–1658–000.

Applicants: Southwest Power Pool, Inc.

Description: Baseline eTariff Filing: Submission of Tariff to Establish Markets+ to be effective 12/31/9998.

Filed Date: 3/29/24.

Accession Number: 20240329–5340.

Comment Date: 5 p.m. ET 4/19/24.

Docket Numbers: ER24–1659–000.

Applicants: Crystal Hill Solar, LLC.

Description: Baseline eTariff Filing: Reactive Power Tariff Application to be effective 3/30/2024.

Filed Date: 3/29/24.

Accession Number: 20240329–5343.

Comment Date: 5 p.m. ET 4/19/24.

Take notice that the Commission received the following electric securities filings:

Docket Numbers: ES24–28–000.

Applicants: PacifiCorp.

Description: Application Under Section 204 of the Federal Power Act for Authorization to Issue Securities of PacifiCorp under.

Filed Date: 3/29/24.

Accession Number: 20240329–5284.

Comment Date: 5 p.m. ET 4/19/24.

The filings are accessible in the Commission's eLibrary system (<https://elibrary.ferc.gov/idmws/search/fercgensearch.asp>) by querying the docket number.

Any person desiring to intervene, to protest, or to answer a complaint in any of the above proceedings must file in accordance with Rules 211, 214, or 206 of the Commission's Regulations (18 CFR 385.211, 385.214, or 385.206) on or before 5:00 p.m. Eastern time on the specified comment date. Protests may be considered, but intervention is necessary to become a party to the proceeding.

eFiling is encouraged. More detailed information relating to filing requirements, interventions, protests, service, and qualifying facilities filings can be found at: <http://www.ferc.gov/docs-filing/efiling/filing-req.pdf>. For other information, call (866) 208–3676 (toll free). For TTY, call (202) 502–8659.

The Commission's Office of Public Participation (OPP) supports meaningful

public engagement and participation in Commission proceedings. OPP can help members of the public, including landowners, environmental justice communities, Tribal members and others, access publicly available information and navigate Commission processes. For public inquiries and assistance with making filings such as interventions, comments, or requests for rehearing, the public is encouraged to contact OPP at (202) 502–6595 or OPP@ferc.gov.

Dated: March 29, 2024.

Debbie-Anne A. Reese,

Acting Secretary.

[FR Doc. 2024–07150 Filed 4–3–24; 8:45 am]

BILLING CODE 6717–01–P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Project Nos. 2341–033 and 2350–025]

Georgia Power Company; Notice of Availability of Environmental Assessment

In accordance with the National Environmental Policy Act of 1969 and the Federal Energy Regulatory Commission's (Commission) regulations, 18 CFR part 380, the Office of Energy Projects has reviewed the application to surrender, decommission, and remove the Langdale Hydroelectric Project No. 2341 and the Riverview Hydroelectric Project No. 2350 (projects). The projects are located on the Chattahoochee River in Chambers County, Alabama and Harris County, Georgia. Commission staff has prepared an Environmental Assessment (EA) for the proposed action.

The EA contains the staff's analysis of the potential environmental effects of the proposed action and concludes that surrendering, decommissioning, and removing the projects, with appropriate environmental protective measures, would not constitute a major federal action that would significantly affect the quality of the human environment.

The Commission provides all interested persons with an opportunity to view and/or print the EA via the internet through the Commission's Home Page (<http://www.ferc.gov/>), using the "eLibrary" link. Enter either docket number (P–2341 or P–2350), to access the document. For assistance, contact FERC Online Support at FERCOnlineSupport@ferc.gov, or at (866) 208–3676 (toll-free), or (202) 502–8659 (TTY).

You may also register online at <https://ferconline.ferc.gov/FERCOOnline.aspx> to be notified via email of new filings and issuances related to this or other pending projects. For assistance, contact FERC Online Support.

The Commission's Office of Public Participation (OPP) supports meaningful public engagement and participation in Commission proceedings. OPP can help members of the public, including landowners, environmental justice communities, Tribal members and others, access publicly available information and navigate Commission processes. For public inquiries and assistance with making filings such as interventions, comments, or requests for rehearing, the public is encouraged to contact OPP at (202) 502-6595, or OPP@ferc.gov.

Any comments must be filed by April 29, 2024.

The Commission strongly encourages electronic filing. Please file comments using the Commission's eFiling system at <https://ferconline.ferc.gov/FERCOOnline.aspx>. Commenters can submit brief comments up to 6,000 characters, without prior registration, using the eComment system at <https://ferconline.ferc.gov/QuickComment.aspx>. You must include your name and contact information at the end of your comments. For assistance, please contact FERC Online Support. In lieu of electronic filing, you may submit a paper copy. Submissions sent via the U.S. Postal Service must be addressed to: Debbie-Anne A. Reese, Acting Secretary, Federal Energy Regulatory Commission, 888 First Street NE, Room 1A, Washington, DC 20426. Submissions sent via any other carrier must be addressed to: Debbie-Anne A. Reese, Acting Secretary, Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, Maryland 20852. The first page of any filing should include docket number P-2341-033 or P-2350-025.

For further information, contact Mark Ivy at 202-502-6156 or mark.ivy@ferc.gov.

Dated: March 29, 2024.

Debbie-Anne A. Reese,
Acting Secretary.

[FR Doc. 2024-07146 Filed 4-3-24; 8:45 am]

BILLING CODE 6717-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Docket Numbers: RP23-1099-000]

Combined Notice of Filings

Take notice that the Commission has received the following Natural Gas Pipeline Rate and Refund Report filings:

Filings Instituting Proceedings

Applicants: Gas Transmission Northwest LLC.

Description: Motion Filing: Section 4 Rate Case Motion to Place Suspended Tariff Records into Effect to be effective 4/1/2024.

Filed Date: 3/28/24.

Accession Number: 20240328-5210.

Comment Date: 5 p.m. ET 4/9/24.

Docket Numbers: RP24-604-000.

Applicants: Eastern Gas Transmission and Storage, Inc.

Description: 4(d) Rate Filing: EGTS—March 28, 2024 Negotiated Rate Agreements to be effective 4/1/2024.

Filed Date: 3/28/24.

Accession Number: 20240328-5175.

Comment Date: 5 p.m. ET 4/9/24.

Docket Numbers: RP24-605-000.

Applicants: Destin Pipeline Company, L.L.C.

Description: 4(d) Rate Filing: Destin Pipeline Negotiated Rate Agreement Filing to be effective 4/1/2024.

Filed Date: 3/28/24.

Accession Number: 20240328-5204.

Comment Date: 5 p.m. ET 4/9/24.

Docket Numbers: RP24-606-000.

Applicants: Millennium Pipeline Company, LLC.

Description: 4(d) Rate Filing: Negotiated Rate Amendment—BKV 210169-2 to be effective 4/1/2024.

Filed Date: 3/28/24.

Accession Number: 20240328-5221.

Comment Date: 5 p.m. ET 4/9/24.

Docket Numbers: RP24-607-000.

Applicants: Portland Natural Gas Transmission System.

Description: 4(d) Rate Filing: Tariff Provision—Operational Purchases and Sales to be effective 4/28/2024.

Filed Date: 3/28/24.

Accession Number: 20240328-5269.

Comment Date: 5 p.m. ET 4/9/24.

Docket Numbers: RP24-608-000.

Applicants: Stagecoach Pipeline & Storage Company LLC.

Description: 4(d) Rate Filing: Negotiated Rate Agreement Filing (Chesapeake) to be effective 4/1/2024.

Filed Date: 3/28/24.

Accession Number: 20240328-5280.

Comment Date: 5 p.m. ET 4/9/24.

Docket Numbers: RP24-609-000.

Applicants: Transcontinental Gas Pipe Line Company, LLC.

Description: 4(d) Rate Filing: Negotiated Rates—FTP—DDC Permt Rls to be effective 2/1/2024.

Filed Date: 3/28/24.

Accession Number: 20240328-5284.

Comment Date: 5 p.m. ET 4/9/24.

Docket Numbers: RP24-610-000.

Applicants: Tennessee Gas Pipeline Company, L.L.C.

Description: 4(d) Rate Filing: Negotiated Rate Agreements Filing—Various Shippers Apr. 2024 to be effective 4/1/2024.

Filed Date: 3/28/24.

Accession Number: 20240328-5303.

Comment Date: 5 p.m. ET 4/9/24.

Docket Numbers: RP24-611-000.

Applicants: Pine Needle LNG Company, LLC.

Description: 4(d) Rate Filing: 2024 Annual Fuel and Electric Power Tracker Filing to be effective 5/1/2024.

Filed Date: 3/29/24.

Accession Number: 20240329-5022.

Comment Date: 5 p.m. ET 4/10/24.

Docket Numbers: RP24-612-000.

Applicants: Kern River Gas Transmission Company.

Description: 4(d) Rate Filing: 2024 Chevron Negotiated Contract 26047 Amendment to be effective 4/1/2024.

Filed Date: 3/29/24.

Accession Number: 20240329-5096.

Comment Date: 5 p.m. ET 4/10/24.

Docket Numbers: RP24-613-000.

Applicants: MountainWest Pipeline, LLC.

Description: 4(d) Rate Filing: Statement of Negotiated Rates V24—Questar Gas 7507 to be effective 4/1/2024.

Filed Date: 3/29/24.

Accession Number: 20240329-5102.

Comment Date: 5 p.m. ET 4/10/24.

Docket Numbers: RP24-614-000.

Applicants: Sabine Pipe Line LLC.

Description: 4(d) Rate Filing: Normal filing 2024—7.26-4.7 to be effective 4/1/2024.

Filed Date: 3/29/24.

Accession Number: 20240329-5124.

Comment Date: 5 p.m. ET 4/10/24.

Docket Numbers: RP24-615-000.

Applicants: Dauphin Island Gathering Partners.

Description: 4(d) Rate Filing: Chevron—Amendment eff 4-1-24 to be effective 4/1/2024.

Filed Date: 3/29/24.

Accession Number: 20240329-5128.

Comment Date: 5 p.m. ET 4/10/24.

Docket Numbers: RP24-616-000.

Applicants: National Fuel Gas Supply Corporation.

Description: Compliance filing: 2024 PS/GHG Costs True-Up Report (GT&C Section 42.3(c)) to be effective N/A.

Filed Date: 3/29/24.

Accession Number: 20240329–5188.

Comment Date: 5 p.m. ET 4/10/24.

Docket Numbers: RP24–617–000.

Applicants: East Tennessee Natural Gas, LLC.

Description: Compliance filing: 2022–2023 ETNG Cashout Report to be effective N/A.

Filed Date: 3/29/24.

Accession Number: 20240329–5208.

Comment Date: 5 p.m. ET 4/10/24.

Any person desiring to intervene, to protest, or to answer a complaint in any of the above proceedings must file in accordance with Rules 211, 214, or 206 of the Commission's Regulations (18 CFR 385.211, 385.214, or 385.206) on or before 5:00 p.m. Eastern time on the specified comment date. Protests may be considered, but intervention is necessary to become a party to the proceeding.

Filings in Existing Proceedings

Docket Numbers: RP23–840–003.

Applicants: Transcontinental Gas Pipe Line Company, LLC.

Description: Compliance filing: Market-Based Rates_Washington Stor SA_Tariff Compliance to be effective 5/1/2024.

Filed Date: 3/29/24.

Accession Number: 20240329–5193.

Comment Date: 5 p.m. ET 4/10/24.

Docket Numbers: RP23–1099–003.

Applicants: Gas Transmission Northwest LLC.

Description: Compliance filing: Section 4 Rate Case Compliance to Place Revised Rates In Effect to be effective 4/1/2024.

Filed Date: 3/28/24.

Accession Number: 20240328–5224.

Comment Date: 5 p.m. ET 4/9/24.

Any person desiring to protest in any of the above proceedings must file in accordance with Rule 211 of the Commission's Regulations (18 CFR 385.211) on or before 5:00 p.m. Eastern time on the specified comment date.

The filings are accessible in the Commission's eLibrary system (<https://elibrary.ferc.gov/idmws/search/fercgensearch.asp>) by querying the docket number.

eFiling is encouraged. More detailed information relating to filing requirements, interventions, protests, service, and qualifying facilities filings can be found at: <http://www.ferc.gov/docs-filing/efiling/filing-req.pdf>. For other information, call (866) 208–3676 (toll free). For TTY, call (202) 502–8659.

The Commission's Office of Public Participation (OPP) supports meaningful public engagement and participation in Commission proceedings. OPP can help

members of the public, including landowners, environmental justice communities, Tribal members and others, access publicly available information and navigate Commission processes. For public inquiries and assistance with making filings such as interventions, comments, or requests for rehearing, the public is encouraged to contact OPP at (202) 502–6595 or OPP@ferc.gov.

Dated: March 29, 2024.

Debbie-Anne A. Reese,

Acting Secretary.

[FR Doc. 2024–07147 Filed 4–3–24; 8:45 am]

BILLING CODE 6717–01–P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Project No. 2705–037]

Seattle City Light; Notice of Availability of Environmental Assessment

In accordance with the National Environmental Policy Act of 1969 and the Federal Energy Regulatory Commission's (Commission or FERC) regulations, 18 CFR part 380, Commission staff reviewed Seattle City Light's (licensee) application for surrender of license for the Newhalem Creek Hydroelectric Project No. 2705 and have prepared an Environmental Assessment (EA) for the proposed surrender. The licensee proposes to decommission and remove most of the project features, including the diversion dam, and to retain certain features considered to be historically important. The project is located on Newhalem Creek, near Newhalem, Whatcom County, Washington. The project occupies federal lands within the Ross Lake National Recreation Area, managed by the National Park Service.

The EA contains Commission staff's analysis of the potential environmental effects of the proposed surrender, alternatives to the proposed action, and concludes that the proposed surrender with appropriate environmental protective measures, would not constitute a major federal action that would significantly affect the quality of the human environment.

The EA may be viewed on the Commission's website at <http://www.ferc.gov> using the "elibrary" link. Enter the docket number (P–2705) in the docket number field to access the document. For assistance, contact FERC Online Support at FERCOnlineSupport@ferc.gov or toll-

free at 1–866–208–3676, or for TTY, (202) 502–8659.

You may also register online at <http://www.ferc.gov/docs-filing/esubscription.asp> to be notified via email of new filings and issuances related to this or other pending projects. For assistance, contact FERC Online Support.

All comments must be filed by April 29, 2024.

The Commission strongly encourages electronic filing. Please file comments using the Commission's eFiling system at <http://www.ferc.gov/docs-filing/efiling.asp>. Commenters can submit brief comments up to 6,000 characters, without prior registration, using the eComment system at <http://www.ferc.gov/docs-filing/ecomment.asp>. You must include your name and contact information at the end of your comments. For assistance, please contact FERC Online Support. In lieu of electronic filing, you may submit a paper copy. Submissions sent via the U.S. Postal Service must be addressed to: Debbie-Anne A. Reese, Acting Secretary, Federal Energy Regulatory Commission, 888 First Street NE, Room 1A, Washington, DC 20426. Submissions sent via any other carrier must be addressed to: Debbie-Anne A. Reese, Acting Secretary, Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, Maryland 20852. The first page of any filing should include docket number P–2705–037.

The Commission's Office of Public Participation (OPP) supports meaningful public engagement and participation in Commission proceedings. OPP can help members of the public, including landowners, environmental justice communities, Tribal members and others, access publicly available information and navigate Commission processes. For public inquiries and assistance with making filings such as interventions, comments, or requests for rehearing, the public is encouraged to contact OPP at (202) 502–6595 or OPP@ferc.gov.

For further information, contact Diana Shannon at 202–502–6136 or diana.shannon@ferc.gov.

Dated: March 29, 2024.

Debbie-Anne A. Reese,

Acting Secretary.

[FR Doc. 2024–07149 Filed 4–3–24; 8:45 am]

BILLING CODE 6717–01–P

DEPARTMENT OF ENERGY**Federal Energy Regulatory Commission**

[Project No. 7153–018]

Consolidated Hydro New York, LLC; Notice of Scoping Meetings and Environmental Site Review and Soliciting Scoping Comments

Take notice that the following hydroelectric application has been filed with the Commission and is available for public inspection.

a. *Type of Application:* New Major License.

b. *Project No.:* 7153–018.

c. *Date filed:* April 29, 2022.

d. *Applicant:* Consolidated Hydro New York, LLC.

e. *Name of Project:* Victory Mills Hydroelectric Project (Victory Mills Project or project).

f. *Location:* On Fish Creek in Saratoga County in the Village of Victory, New York.

g. *Filed Pursuant to:* Federal Power Act, 16 U.S.C. 791(a)–825(r).

h. *Applicant Contact:* Curtis Mooney, Manager, Regulatory Affairs, Patriot Hydro, LLC, 59 Ayers Island Road, Bristol, NH 03222, (603) 744–0846, or, Kevin Webb, Hydro Licensing Manager, Patriot Hydro, LLC, 670 N Commercial Street, Suite 204, Manchester, NH 03101, (603) 623–8222.

i. *FERC Contact:* Jacob Harrell, jacob.harrell@ferc.gov, (202) 502–7313.

j. *Deadline for filing scoping comments:* May 30, 2024.

The Commission strongly encourages electronic filing. Please file scoping comments using the Commission's eFiling system at <https://ferconline.ferc.gov/FERCOOnline.aspx>. Commenters can submit brief comments up to 6,000 characters, without prior registration, using the eComment system at <https://ferconline.ferc.gov/QuickComment.aspx>. You must include your name and contact information at the end of your comments. For assistance, please contact FERC Online Support at FERCOOnlineSupport@ferc.gov, (866) 208–3676 (toll free), or (202) 502–8659 (TTY). In lieu of electronic filing, please send a paper copy via U.S. Postal Service to: Debbie-Anne A. Reese, Acting Secretary, Federal Energy Regulatory Commission, 888 First Street NE, Room 1A, Washington, DC 20426. Submissions sent via any other carrier must be addressed to: Debbie-Anne A. Reese, Acting Secretary, Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, Maryland 20852. All filings must clearly identify the project name and docket number on the first

page: Victory Mills Hydroelectric Project (P–7153–018).

The Commission's Rules of Practice and Procedure require all interveners filing documents with the Commission to serve a copy of that document on each person on the official service list for the project. Further, if an intervenor files comments or documents with the Commission relating to the merits of an issue that may affect the responsibilities of a particular resource agency, they must also serve a copy of the document on that resource agency.

k. This application is not ready for environmental analysis at this time.

1. *The Victory Mills Project consists of:*

(1) a dam that includes: (a) an approximately 150-foot-long concrete spillway varying in height from 4 to 6 feet with a crest elevation of 187.5 feet National Geodetic Vertical Datum of 1929 (NGVD29), and (b) a sluice gate section approximately 19 feet high and 40 feet long with four gated spillway bays, each with a sill elevation of 181 feet NGVD29 and containing a 7-foot-high by 8-foot-wide wooden timber gate; (2) a 4.3-acre reservoir with a gross storage capacity of approximately 18 acre-feet at the normal surface elevation of 187.5 feet NGVD29; (3) an intake channel feeding a 51-foot-long, 25-foot-high concrete intake structure; (4) an 8-foot-diameter, 300-foot-long steel penstock; (5) a 27-foot by 46-foot concrete powerhouse containing a single turbine-generator unit with an installed capacity of 1,656 kilowatts; (6) an approximately 30-foot-wide by 530-foot-long tailrace channel; (7) a 90-foot-long generator lead extending through the powerhouse to a transformer and then a 100-foot-long underground and a 20-foot-long aerial, 4.16-kilovolt transmission line to the point of interconnection; and (8) appurtenant facilities. There are no recreation facilities at the project. An average of 6,073 MWh is generated at the project annually.

The Victory Mills Project operates as a run-of-river facility with no storage or flood control capacity. A continuous minimum bypassed reach flow of 36 cubic feet per second (cfs), or inflow, whichever is less, is maintained through operation of a sluice gate at the dam. The minimum hydraulic capacity for operating the turbine unit is 60 cfs, therefore, the minimum river flow needed for project operation is 96 cfs (36 cfs plus 60 cfs). When inflow at the project is less than 96 cfs, river flows are allowed to pass downstream through the bypassed reach. When the inflow exceeds the maximum hydraulic capacity of the project at 590 cfs, the

impoundment level is permitted to rise over the spillway.

m. Copies of the application can be viewed on the Commission's website at <https://www.ferc.gov>, using the "eLibrary" link. Enter the project's docket number, excluding the last three digits in the docket number field, to access the document. For assistance, contact FERC Online Support.

You may also register online at <http://www.ferc.gov/docs-filing/esubscription.asp> to be notified via email of new filings and issuances related to this or other pending projects. For assistance, contact FERC Online Support.

The Commission's Office of Public Participation (OPP) supports meaningful public engagement and participation in Commission proceedings. OPP can help members of the public, including landowners, environmental justice communities, Tribal members and others, access publicly available information and navigate Commission processes. For public inquiries and assistance with making filings such as interventions, comments, or requests for rehearing, the public is encouraged to contact OPP at (202) 502–6595, or at OPP@ferc.gov.

n. *Scoping Process*

Pursuant to the National Environmental Policy Act (NEPA), Commission staff intends to prepare either an environmental assessment (EA) or an environmental impact statement (EIS) (collectively referred to as the "NEPA document") that describes and evaluates the probable effects, including an assessment of the site-specific and cumulative effects, if any, of the proposed action and alternatives. The Commission's scoping process will help determine the required level of analysis and satisfy the NEPA scoping requirements, irrespective of whether the Commission issues an EA or an EIS.

Scoping Meetings

Commission staff will hold two public scoping meetings and an environmental site review in the vicinity of the project to receive input on the scope of the NEPA document. An evening meeting will focus on receiving input from the public and a daytime meeting will focus on the concerns of resource agencies, non-governmental organizations (NGOs), and Indian Tribes. We invite all interested agencies, Indian Tribes, NGOs, and individuals to attend one or both meetings. The times and locations of these meetings are as follows:

Evening Scoping Meeting

Date: Monday, April 29, 2024

Time: 7:00 p.m. EDT

Place: Village of Victory Town Hall
Address: 23 Pine Street, Victory Mills,
NY 12884

Daytime Scoping Meeting

Date: Tuesday, April 30, 2024
Time: 9:00 a.m. EDT

Place: Village of Victory Town Hall
Address: 23 Pine Street, Victory Mills,
NY 12884

Copies of the Scoping Document (SD1) outlining the subject areas to be addressed in the NEPA document were distributed to the parties on the Commission's mailing list. Copies of the SD1 will be available at the scoping meeting or may be viewed on the web at <http://www.ferc.gov> using the "eLibrary" link (see item m above).

Environmental Site Review

The applicant and Commission staff will conduct an environmental site review of the project. All interested individuals, agencies, Indian Tribes, and NGOs are invited to attend. All participants are responsible for their own transportation to the site. Please RSVP via email to Miley Kinney at Mkinney@patriohydro.com or by phone at (603) 732-8162 by April 19, 2024, if you plan to attend the environmental site review. The time and location of the environmental site review is as follows:

Date: Tuesday, April 30, 2024

Time: 1:00 p.m. EDT

Place: Village of Victory Town Hall
Address: 23 Pine Street, Victory Mills,
NY 12884

All persons attending the environmental site review must adhere to the following requirements: (1) all persons must wear sturdy, closed-toe shoes or boots; (2) persons with open-toed shoes/sandals/flip flops/high heels, etc. will not be allowed on the environmental site review; (3) persons must be 18 years or older; (4) no photography will be allowed inside the powerhouse; (5) no weapons are allowed on-site; (6) no alcohol/drugs are allowed on-site (or persons exhibiting the effects thereof); and (7) no animals (except for service animals) are allowed on the environmental site review.

Objectives

At the scoping meetings, Commission staff will: (1) summarize the environmental issues tentatively identified for analysis in the NEPA document; (2) solicit from the meeting participants all available information, especially quantifiable data, on the resources at issue; (3) encourage statements from experts and the public on issues that should be analyzed in the NEPA document, including viewpoints

in opposition to, or in support of, the staff's preliminary views; (4) determine the resource issues to be addressed in the NEPA document; and (5) identify those issues that require a detailed analysis, as well as those issues that do not require a detailed analysis.

Procedures

The meetings are recorded by a stenographer and become part of the formal record of the Commission proceeding on the project. Individuals, NGOs, Indian Tribes, and agencies with environmental expertise and concerns are encouraged to attend the meeting and to assist the staff in defining and clarifying the issues to be addressed in the NEPA document.

Dated: March 29, 2024.

Debbie-Anne A. Reese,

Acting Secretary.

[FR Doc. 2024-07148 Filed 4-3-24; 8:45 am]

BILLING CODE 6717-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

[Document Identifiers: CMS-18F5 and CMS-10537]

Agency Information Collection Activities: Proposed Collection; Comment Request

AGENCY: Centers for Medicare & Medicaid Services, Health and Human Services (HHS).

ACTION: Notice.

SUMMARY: The Centers for Medicare & Medicaid Services (CMS) is announcing an opportunity for the public to comment on CMS' intention to collect information from the public. Under the Paperwork Reduction Act of 1995 (PRA), Federal agencies are required to publish notice in the **Federal Register** concerning each proposed collection of information (including each proposed extension or reinstatement of an existing collection of information) and to allow 60 days for public comment on the proposed action. Interested persons are invited to send comments regarding our burden estimates or any other aspect of this collection of information, including the necessity and utility of the proposed information collection for the proper performance of the agency's functions, the accuracy of the estimated burden, ways to enhance the quality, utility, and clarity of the information to be collected, and the use of automated collection techniques or other forms of

information technology to minimize the information collection burden.

DATES: Comments must be received by June 3, 2024.

ADDRESSES: When commenting, please reference the document identifier or OMB control number. To be assured consideration, comments and recommendations must be submitted in any one of the following ways:

1. *Electronically.* You may send your comments electronically to <http://www.regulations.gov>. Follow the instructions for "Comment or Submission" or "More Search Options" to find the information collection document(s) that are accepting comments.

2. *By regular mail.* You may mail written comments to the following address: CMS, Office of Strategic Operations and Regulatory Affairs, Division of Regulations Development, Attention: Document Identifier/OMB Control Number: _____, Room C4-26-05, 7500 Security Boulevard, Baltimore, Maryland 21244-1850.

To obtain copies of a supporting statement and any related forms for the proposed collection(s) summarized in this notice, please access the CMS PRA website by copying and pasting the following web address into your web browser: <https://www.cms.gov/Regulations-and-Guidance/Legislation/PaperworkReductionActof1995/PRA-Listing>.

FOR FURTHER INFORMATION CONTACT: William N. Parham at (410) 786-4669.

SUPPLEMENTARY INFORMATION:

Contents

This notice sets out a summary of the use and burden associated with the following information collections. More detailed information can be found in each collection's supporting statement and associated materials (see **ADDRESSES**).

CMS-18F5 Application for Enrollment in Medicare Part A internet Claim (iClaim) Application Screen Modernized Claims System and Consolidated Claim Experience Screens Survey Form

CMS-10537 CAHPS Hospice Survey

Under the PRA (44 U.S.C. 3501-3520), Federal agencies must obtain approval from the Office of Management and Budget (OMB) for each collection of information they conduct or sponsor. The term "collection of information" is defined in 44 U.S.C. 3502(3) and 5 CFR 1320.3(c) and includes agency requests or requirements that members of the public submit reports, keep records, or provide information to a third party.

Section 3506(c)(2)(A) of the PRA requires Federal agencies to publish a 60-day notice in the **Federal Register** concerning each proposed collection of information, including each proposed extension or reinstatement of an existing collection of information, before submitting the collection to OMB for approval. To comply with this requirement, CMS is publishing this notice.

Information Collection

1. Type of Information Collection

Request: Extension without change of a currently approved collection; *Title of Information Collection:* Application for Enrollment in Medicare Part A Internet Claim (iClaim) Application Screen Modernized Claims System and Consolidated Claim Experience Screens; *Use:* The Centers for Medicare and Medicaid Services (CMS) Form “Application for Hospital Insurance” supports sections 1818 and 1818A of the Social Security Act (the Act) and corresponding regulations at 42 CFR 406.6 and 406.7.

The CMS–18–F5 is used to establish entitlement to Part A and enrollment in Part B for claimants who must file an application. The application follows the questions and requirements used by SSA on the electronic application. This is done not only for consistency purposes but because certain requirements under titles II and XVIII of the act must be met in order to qualify for Part A and Part B; including insured status, relationship and residency. The form is owned by CMS but is not utilized by CMS staff. SSA uses the form to collect information and make Part A and Part B entitlement determinations on behalf of CMS. *Form Number:* CMS–18F5 (OMB control number: 0938–0251); *Frequency:* Once; *Affected Public:* Individuals and Households; *Number of Respondents:* 1,042,263; *Total Annual Responses:* 1,042,263; *Total Annual Hours:* 260,566. (For policy questions regarding this collection contact Carla Patterson at 410–786–8911 or Carla.Patterson@cms.hhs.gov).

2. Type of Information Collection

Request: Revision of a currently approved collection; *Title of Information Collection:* CAHPS Hospice Survey; *Use:* CMS launched the development of the CAHPS Hospice Survey in 2012. Public reporting of the results on Hospice Compare started in 2018. The goal of the survey is to measure the experiences of patients and their caregivers with hospice care. The survey was developed to:

- Provide a source of information from which selected measures could be

publicly reported to beneficiaries and their family members as a decision aid for selection of a hospice program;

- Aid hospices with their internal quality improvement efforts and external benchmarking with other facilities; and
- Provide CMS with information for monitoring the care provided.

Surveys focusing on patients’ experience of care with their health care providers are an important part of the NQS. In addition to publicly reporting clinical quality measures, CMS is currently reporting measures from patient experience of care surveys in a variety of settings, including in-center hemodialysis (ICH) centers, hospitals, home health agencies, and hospices on the Medicare Care Compare website. (<https://www.medicare.gov/care-compare>). *Form Number:* CMS–10537 (OMB control number: 0938–1257); *Frequency:* Once; *Affected Public:* Individuals and Households; *Number of Respondents:* 1,159,420; *Total Annual Responses:* 1,159,420; *Total Annual Hours:* 168,115.90. (For policy questions regarding this collection contact Lauren Fuentes at 410–786–2290 or 443–618–2123).

William N. Parham, III,

Director, Division of Information Collections and Regulatory Impacts, Office of Strategic Operations and Regulatory Affairs.

[FR Doc. 2024–07162 Filed 4–3–24; 8:45 am]

BILLING CODE 4120–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. FDA–2024–D–0706]

New Dietary Ingredient Notification Master Files for Dietary Supplements; Draft Guidance for Industry; Availability; Agency Information Collection Activities; Comment Request

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice of availability.

SUMMARY: The Food and Drug Administration (FDA or we) is announcing the availability of a draft guidance for industry entitled “New Dietary Ingredient Notification Master Files for Dietary Supplements.” The draft guidance, when finalized, will provide recommendations to the dietary supplement industry on Master Files for new dietary ingredients. The purpose of this draft guidance, when finalized, will be to help industry comply more easily with the new dietary ingredient

notification requirement by providing recommendations on the submission and use of Master Files that contain identity, manufacturing, or safety data that can be used to support a new dietary ingredient notification. New dietary ingredient Master Files are submitted solely at the discretion of the Master File owner and are not required by statute or regulation.

DATES: Submit either electronic or written comments on the draft guidance by June 3, 2024 to ensure that we consider your comment on the draft guidance before we begin work on the final version of the guidance.

ADDRESSES: You may submit comments on any guidance at any time as follows:

Electronic Submissions

Submit electronic comments in the following way:

- *Federal eRulemaking Portal:* <https://www.regulations.gov>. Follow the instructions for submitting comments. Comments submitted electronically, including attachments, to <https://www.regulations.gov> will be posted to the docket unchanged. Because your comment will be made public, you are solely responsible for ensuring that your comment does not include any confidential information that you or a third party may not wish to be posted, such as medical information, your or anyone else’s Social Security number, or confidential business information, such as a manufacturing process. Please note that if you include your name, contact information, or other information that identifies you in the body of your comments, that information will be posted on <https://www.regulations.gov>.

- If you want to submit a comment with confidential information that you do not wish to be made available to the public, submit the comment as a written/paper submission and in the manner detailed (see “Written/Paper Submissions” and “Instructions”).

Written/Paper Submissions

Submit written/paper submissions as follows:

- *Mail/Hand Delivery/Courier (for written/paper submissions):* Dockets Management Staff (HFA–305), Food and Drug Administration, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852.
- For written/paper comments submitted to the Dockets Management Staff, FDA will post your comment, as well as any attachments, except for information submitted, marked and identified, as confidential, if submitted as detailed in “Instructions.”

Instructions: All submissions received must include the Docket No. FDA–

2024–D–0706 for “New Dietary Ingredient Notification Master Files for Dietary Supplements.” Received comments will be placed in the docket and, except for those submitted as “Confidential Submissions,” publicly viewable at <https://www.regulations.gov> or at the Dockets Management Staff between 9 a.m. and 4 p.m., Monday through Friday, 240–402–7500.

- Confidential Submissions—To submit a comment with confidential information that you do not wish to be made publicly available, submit your comments only as a written/paper submission. You should submit two copies total. One copy will include the information you claim to be confidential with a heading or cover note that states “THIS DOCUMENT CONTAINS CONFIDENTIAL INFORMATION.” We will review this copy, including the claimed confidential information, in our consideration of comments. The second copy, which will have the claimed confidential information redacted/blacked out, will be available for public viewing and posted on <https://www.regulations.gov>. Submit both copies to the Dockets Management Staff. If you do not wish your name and contact information to be made publicly available, you can provide this information on the cover sheet and not in the body of your comments and you must identify this information as “confidential.” Any information marked as “confidential” will not be disclosed except in accordance with 21 CFR 10.20 and other applicable disclosure law. For more information about FDA’s posting of comments to public dockets, see 80 FR 56469, September 18, 2015, or access the information at: <https://www.govinfo.gov/content/pkg/FR-2015-09-18/pdf/2015-23389.pdf>.

Docket: For access to the docket to read background documents or the electronic and written/paper comments received, go to <https://www.regulations.gov> and insert the docket number, found in brackets in the heading of this document, into the “Search” box and follow the prompts and/or go to the Dockets Management Staff, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852, 240–402–7500.

You may submit comments on any guidance at any time (see 21 CFR 10.115(g)(5)).

Submit written requests for single copies of the draft guidance to the Office of Dietary Supplement Programs, Center for Food Safety and Applied Nutrition, Food and Drug Administration, 5001 Campus Dr., College Park, MD 20740. Send two self-addressed adhesive labels to assist that office in processing your request. See the **SUPPLEMENTARY**

INFORMATION section for electronic access to the draft guidance.

FOR FURTHER INFORMATION CONTACT: Lisa Bieniek, Office of Dietary Supplement Programs (HFS–810), Center for Food Safety and Applied Nutrition, Food and Drug Administration, 5001 Campus Dr., College Park, MD 20740, 240–402–2371; or Lauren Kleinman, Office of Regulations and Policy (HFS–024), Center for Food Safety and Applied Nutrition, Food and Drug Administration, 5001 Campus Dr., College Park, MD 20740, 240–402–2378.

SUPPLEMENTARY INFORMATION:

I. Background

FDA is announcing the availability of a draft guidance for industry titled, “New Dietary Ingredient Notification Master Files for Dietary Supplements.” We are issuing the draft guidance consistent with our good guidance practices regulation (21 CFR 10.115). The draft guidance, when finalized, will represent the current thinking of FDA on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternate approach if it satisfies the requirements of the applicable statutes and regulations.

The draft guidance, when finalized, will provide recommendations to industry on Master Files for new dietary ingredient notifications (NDINs). For purposes of the guidance, a new dietary ingredient notification Master File (NDIN Master File or Master File) is a file containing identity, manufacturing, and/or safety information relating to a new dietary ingredient (NDI) that the Master File owner submits to FDA for use in evaluating a potential future NDIN by the Master File owner or by another person designated by the Master File owner (e.g., business partner, supplement manufacturer). An NDIN Master File contains information about an NDI, a dietary supplement containing an NDI, or both. The Master File owner may refer to the Master File in an NDIN or may grant written authorization to other parties to incorporate information from the Master File by reference in NDINs. A written authorization granting a right of reference to a Master File in an NDIN does not include the right to see or copy the Master File.

The recommendations in this draft guidance expand upon and replace the recommendations related to Master Files in FDA’s revised draft guidance, “Dietary Supplements: New Dietary Ingredient Notifications and Related Issues,” dated August 2016. The purpose of this draft guidance, when finalized, will be to help industry

comply more easily with the NDIN requirement in the Federal Food, Drug, and Cosmetic Act (FD&C Act) by providing recommendations for the submission and use of NDIN Master Files (see section 413(a)(2) of the FD&C Act (21 U.S.C. 350b(a)(2))). The draft guidance contains information on establishing an NDIN Master File, updating or closing an NDIN Master File, the use of data from an NDIN Master File by the Master File owner and other parties authorized by the Master File owner, and FDA’s role in reviewing and administering NDIN Master Files. Master Files benefit NDIN submitters with a right of reference by allowing them to refer to data already on file with FDA, instead of having to develop the data themselves and resubmit it in each NDIN for the same ingredient.

II. Paperwork Reduction Act of 1995

While this guidance contains no collection of information, it does refer to previously approved FDA collections of information. The previously approved collections of information are subject to review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501–3521). The collection of information in 21 CFR 190.6 has been approved under OMB control number 0910–0330, and the collections of information in 21 CFR part 111 have been approved under OMB control number 0910–0606.

III. Electronic Access

Persons with access to the internet may obtain the draft guidance at either <https://www.fda.gov/regulatory-information/search-fda-guidance-documents> or <https://www.regulations.gov>. Use the FDA website listed in the previous sentence to find the most current version of the guidance.

Dated: March 28, 2024.

Lauren K. Roth,

Associate Commissioner for Policy.

[FR Doc. 2024–07095 Filed 4–3–24; 8:45 am]

BILLING CODE 4164–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Institute of Biomedical Imaging and Bioengineering; Notice of Meeting

Pursuant to section 1009 of the Federal Advisory Committee Act, as amended, notice is hereby given of a

meeting of the National Advisory Council for Biomedical Imaging and Bioengineering.

The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Advisory Council for Biomedical Imaging and Bioengineering (NACBIB).

Date: May 15, 2024.

Open: 09:00 a.m. to 12:30 p.m.

Agenda: Report from the Institute Director, Council Members and other Institute Staff.

Place: John Edward Porter Neuroscience Research Center, Building 35A, Room 620/630, 35 Convent Drive, Bethesda, Maryland 20892 (In-person Meeting).

Closed: 1:30 p.m. to 4:00 p.m.

Agenda: To review and evaluate grant applications and/or proposals.

Place: John Edward Porter Neuroscience Research Center, Building 35A, Room 620/630, 35 Convent Drive, Bethesda, Maryland 20892 (In-person Meeting).

Contact Person: David T. George, Ph.D., Associate Director for Research Administration, Office of Research Administration, National Institute of Biomedical Imaging and Bioengineering, 6707 Democracy Boulevard, Bethesda, MD 20892, georged@mail.nih.gov.

The meeting will be open to the public, with attendance limited to space available. Individuals who plan to attend and need special assistance, such as sign language interpretation or other reasonable accommodations, should notify the Contact Person listed below in advance of the meeting. In person attendees should register at (<https://www.nibib.nih.gov/about-nibib/advisory-council>) in advance of the meeting so that the meeting organizers can plan accordingly.

The meeting will be videocast and can be accessed from the NIH Videocasting website at (<https://videocast.nih.gov/watch=54286>).

Any interested person may file written comments with the committee by forwarding the statement to the Contact Person listed on this notice. The statement should include the name, address, telephone number and when applicable, the business or professional affiliation of the interested person.

Information is also available on the Institute's/Center's home page: <https://www.nibib.nih.gov/about-nibib/advisory-council> where an agenda and any additional information for the meeting will be posted when available.

Dated: March 29, 2024.

Miguelina Perez,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2024-07112 Filed 4-3-24; 8:45 am]

BILLING CODE 4140-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Institute of Diabetes and Digestive and Kidney Diseases; Notice of Meeting

Pursuant to section 1009 of the Federal Advisory Committee Act, as amended, notice is hereby given of a meeting of the National Diabetes and Digestive and Kidney Diseases Advisory Council.

The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Institute of Diabetes and Digestive and Kidney Diseases Special Emphasis Panel; RFA-DK-22-028 Pilot and Feasibility Trials on the Integration of Social and Medical Care for T1D.

Date: June 7, 2024.

Time: 12:00 p.m. to 2:00 p.m.

Agenda: To review and evaluate grant applications.

Place: National Institutes of Health, NIDDK, Democracy II, Suite 7000A, 6707 Democracy Boulevard, Bethesda, MD 20892 (Virtual Meeting).

Contact Person: Cheryl Nordstrom, Ph.D., Scientific Review Officer, Review Branch, DEA, NIDDK, National Institutes of Health, Room 7013, 6707 Democracy Blvd., Bethesda, MD 20892-2542, 301-402-6711, cheryl.nordstrom@nih.gov.

(Catalogue of Federal Domestic Assistance Program Nos. 93.847, Diabetes, Endocrinology and Metabolic Research; 93.848, Digestive Diseases and Nutrition Research; 93.849, Kidney Diseases, Urology and Hematology Research, National Institutes of Health, HHS)

Dated: April 1, 2024.

Miguelina Perez,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2024-07156 Filed 4-3-24; 8:45 am]

BILLING CODE 4140-01-P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG-2024-0232]

National Maritime Security Advisory Committee; May 2024 Virtual Meeting

AGENCY: U.S. Coast Guard, Department of Homeland Security.

ACTION: Notice of open Federal advisory committee meeting.

SUMMARY: The National Maritime Security Advisory Committee (Committee) will conduct a virtual meeting to discuss a new Committee task to provide Comment on the U.S. Coast Guard's Notice of Proposed Rulemaking on Cybersecurity in the Marine Transportation System. The virtual meeting will be open to the public.

DATES:

Meeting: The Committee will meet virtually on Friday, May 10, 2024, from 1 p.m. until 3 p.m. Eastern Daylight Time (EDT). Please note that this meeting may close early if the Committee has completed its business.

Comments and supporting documentation: To ensure your comments are received by Committee members before the meeting, submit your written comments no later than May 9, 2024.

ADDRESSES: The meeting will be held virtually. To join the virtual meeting or to request special accommodations, contact the individual listed in the **FOR FURTHER INFORMATION CONTACT** section no later than 1 p.m. EDT on May 9, 2024, to obtain the needed information. The number of virtual lines are limited and will be available on a first-come, first-served basis.

Pre-registration information: Pre-registration is required for attending virtual meeting. You must request attendance by contacting the individual listed in the **FOR FURTHER INFORMATION CONTACT** section of this notice. You will receive a response with attendance instructions.

The National Maritime Security Advisory Committee is committed to ensuring all participants have equal access regardless of disability status. If you require reasonable accommodations due to a disability to fully participate, please email Mr. Ryan Owens at ryan.f.owens.uscg.mil or call (202) 302-6565 as soon as possible.

Instructions: You are free to submit comments at any time, including orally at the meetings as time permits, but if you want Committee members to review

your comment before the meetings, please submit your comments no later than May 9, 2024. We are particularly interested in comments regarding the topics in the “Agenda” section below. We encourage you to submit comments through Federal Decision-Making Portal at <https://www.regulations.gov>. To do so, go to <https://www.regulations.gov>, type USCG–2024–0232 in the search box and click “Search”. Next, look for this notice in the Search Results column, and click on it. Then click on the Comment option. If your material cannot be submitted using <https://www.regulations.gov>, email the individual in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions. You must include the docket number USCG–2024–0232. Comments received will be posted without alteration at <https://www.regulations.gov> including any personal information provided. You may wish to review the Privacy and Security Notice found via a link on the homepage <https://www.regulations.gov>. For more about the privacy and submissions in response to this document, see DHS’s eRulemaking System of Records notice (85 FR 14226, March 11, 2020). If you encounter technical difficulties with comment submission, contact the individual listed in the **FOR FURTHER INFORMATION CONTACT** section of this notice.

Docket Search: Documents mentioned in this notice as being available in the docket, and all public comments, will be in our online docket at <https://www.regulations.gov>, and can be viewed by following that website’s instructions. Additionally, if you go to the online docket and sign-up for email alerts, you will be notified when comments are posted.

FOR FURTHER INFORMATION CONTACT: Mr. Ryan Owens, Alternate Designated Federal Officer of the National Maritime Security Advisory Committee, telephone 202–302–6565 or email at ryan.f.owens@uscg.mil.

SUPPLEMENTARY INFORMATION: Notice of this meeting is in compliance with the *Federal Advisory Committee Act*, (Pub. L. 117–286, 5 U.S.C. ch. 10). The Committee was established by section 601 of the *Frank LoBiondo Coast Guard Authorization Act of 2018*, (Pub. L. 115–282, 132 Stat. 4190) and is codified in 46 U.S.C. 70112(a). The Committee operates under the provisions of the *Federal Advisory Committee Act* and 46 U.S.C. 15109. The National Maritime Security Advisory Committee provides advice, consults with, and makes recommendations to the Secretary of Homeland Security, via the

Commandant of the U.S. Coast Guard, on matters relating to national maritime security.

Agenda

Friday, May 10, 2024

- (1) Call to Order.
- (2) Introduction.
- (3) Designated Federal Officer Remarks.
- (4) Roll call of Committee Members and Determination of Quorum.
- (5) Remarks from Committee Leadership.
- (6) Presentation of Task T–2024–1: Notice of Proposed Rulemaking on Cybersecurity in the Marine Transportation System.
- (7) Public Comment Period.
- (8) Meeting Adjournment.

A copy of all meeting documentation will be available at <https://homeport.uscg.mil/NMSAC> no later than May 3, 2024. Alternatively, you may contact Mr. Ryan Owens as noted in the **FOR FURTHER INFORMATION CONTACT** section above. There will be a public comment period at the end of meetings. Speakers are requested to limit their comments to 3 minutes. Please note that the public comment period may end before the period allotted, following the last call for comments. Please contact the individual listed in the **FOR FURTHER INFORMATION CONTACT** section above to register as a speaker.

Dated: March 29, 2024.

Amy M. Beach,

Captain, U.S. Coast Guard, Director of Inspections and Compliance.

[FR Doc. 2024–07097 Filed 4–3–24; 8:45 am]

BILLING CODE 9110–04–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG–2024–0238]

Information Collection Request to Office of Management and Budget; OMB Control Number: 1625–0073

AGENCY: Coast Guard, DHS.

ACTION: Sixty-day notice requesting comments.

SUMMARY: In compliance with the Paperwork Reduction Act of 1995, the U.S. Coast Guard intends to submit an Information Collection Request (ICR) to the Office of Management and Budget (OMB), Office of Information and Regulatory Affairs (OIRA), requesting an extension of its approval for the following collection of information: 1625–0073, Alteration of Unreasonable Obstructive Bridges; without change.

Our ICR describes the information we seek to collect from the public. Before submitting this ICR to OIRA, the Coast Guard is inviting comments as described below.

DATES: Comments must reach the Coast Guard on or before June 3, 2024.

ADDRESSES: You may submit comments identified by Coast Guard docket number [USCG–2024–0238] to the Coast Guard using the Federal eRulemaking Portal at <https://www.regulations.gov>. See the “Public participation and request for comments” portion of the **SUPPLEMENTARY INFORMATION** section for further instructions on submitting comments.

A copy of the ICR is available through the docket on the internet at <https://www.regulations.gov>. Additionally, copies are available from: Commandant (CG–6P), Attn: Paperwork Reduction Act Manager, U.S. Coast Guard, 2703 Martin Luther King Jr. Ave. SE, Stop 7710, Washington, DC 20593–7710.

FOR FURTHER INFORMATION CONTACT: A.L. Craig, Office of Privacy Management, telephone 202–475–3528, fax 202–372–8405, or email hqs-dg-m-cg-61-pii@uscg.mil for questions on these documents.

SUPPLEMENTARY INFORMATION:

Public Participation and Request for Comments

This notice relies on the authority of the Paperwork Reduction Act of 1995; 44 U.S.C. 3501 *et seq.*, chapter 35, as amended. An ICR is an application to OIRA seeking the approval, extension, or renewal of a Coast Guard collection of information (Collection). The ICR contains information describing the Collection’s purpose, the Collection’s likely burden on the affected public, an explanation of the necessity of the Collection, and other important information describing the Collection. There is one ICR for each Collection.

The Coast Guard invites comments on whether this ICR should be granted based on the Collection being necessary for the proper performance of Departmental functions. In particular, the Coast Guard would appreciate comments addressing: (1) the practical utility of the Collection; (2) the accuracy of the estimated burden of the Collection; (3) ways to enhance the quality, utility, and clarity of information subject to the Collection; and (4) ways to minimize the burden of the Collection on respondents, including the use of automated collection techniques or other forms of information technology.

In response to your comments, we may revise this ICR or decide not to seek

an extension of approval for the Collection. We will consider all comments and material received during the comment period.

We encourage you to respond to this request by submitting comments and related materials. Comments must contain the OMB Control Number of the ICR and the docket number of this request, USCG–2024–0238, and must be received by June 3, 2024.

Submitting Comments

We encourage you to submit comments through the Federal eRulemaking Portal at <https://www.regulations.gov>. If your material cannot be submitted using <https://www.regulations.gov>, contact the person in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions. Documents mentioned in this notice, and all public comments, are in our online docket at <https://www.regulations.gov> and can be viewed by following that website's instructions. Additionally, if you go to the online docket and sign up for email alerts, you will be notified when comments are posted.

We accept anonymous comments. All comments received will be posted without change to <https://www.regulations.gov> and will include any personal information you have provided. For more about privacy and submissions in response to this document, see DHS's eRulemaking System of Records notice (85 FR 14226, March 11, 2020).

Title: Alteration of Unreasonable Obstructive Bridges.

OMB Control Number: 1625–0073.

Summary: The collection of information is a request to determine if the bridge is unreasonably obstructive.

Need: 33 U.S.C. 494, 502, 511, 513, 514, 515 516, 517, 521, 522, 523 and 524 authorize the Coast Guard to require the removal or alteration of bridges and causeways over the navigable waters of the United States and that the Coast Guard deems to be unreasonably obstructive.

Forms: None.

Respondents: Public and private owners of bridges over navigable waters of the United States.

Frequency: On occasion.

Hour Burden Estimate: The estimated burden remains 160 hours a year.

Authority: The Paperwork Reduction Act of 1995; 44 U.S.C. chapter 35, as amended.

Dated: March 29, 2024.

Kathleen Claffie,

Chief, Office of Privacy Management, U.S. Coast Guard.

[FR Doc. 2024–07125 Filed 4–3–24; 8:45 am]

BILLING CODE 9110–04–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG–2024–0239]

Information Collection Request to Office of Management and Budget; OMB Control Number: 1625–0106

AGENCY: Coast Guard, DHS.

ACTION: Sixty-day notice requesting comments.

SUMMARY: In compliance with the Paperwork Reduction Act of 1995, the U.S. Coast Guard intends to submit an Information Collection Request (ICR) to the Office of Management and Budget (OMB), Office of Information and Regulatory Affairs (OIRA), requesting an extension of its approval for the following collection of information: 1625–0106, Unauthorized Entry into Cuban Territorial Waters; without change.

Our ICR describes the information we seek to collect from the public. Before submitting this ICR to OIRA, the Coast Guard is inviting comments as described below.

DATES: Comments must reach the Coast Guard on or before June 3, 2024.

ADDRESSES: You may submit comments identified by Coast Guard docket number [USCG–2024–0239] to the Coast Guard using the Federal eRulemaking Portal at <https://www.regulations.gov>. See the “Public participation and request for comments” portion of the **SUPPLEMENTARY INFORMATION** section for further instructions on submitting comments.

A copy of the ICR is available through the docket on the internet at <https://www.regulations.gov>. Additionally, copies are available from: Commandant (CG–6P), Attn: Paperwork Reduction Act Manager, U.S. Coast Guard, 2703 Martin Luther King Jr. Ave. SE, Stop 7710, Washington, DC 20593–7710.

FOR FURTHER INFORMATION CONTACT: A.L. Craig, Office of Privacy Management, telephone 202–475–3528, fax 202–372–8405, or email hqs-dg-m-cg-61-pii@uscg.mil for questions on these documents.

SUPPLEMENTARY INFORMATION:

Public Participation and Request for Comments

This notice relies on the authority of the Paperwork Reduction Act of 1995; 44 U.S.C. 3501 *et seq.*, chapter 35, as amended. An ICR is an application to OIRA seeking the approval, extension, or renewal of a Coast Guard collection of information (Collection). The ICR contains information describing the Collection's purpose, the Collection's likely burden on the affected public, an explanation of the necessity of the Collection, and other important information describing the Collection. There is one ICR for each Collection.

The Coast Guard invites comments on whether this ICR should be granted based on the Collection being necessary for the proper performance of Departmental functions. In particular, the Coast Guard would appreciate comments addressing: (1) the practical utility of the Collection; (2) the accuracy of the estimated burden of the Collection; (3) ways to enhance the quality, utility, and clarity of information subject to the Collection; and (4) ways to minimize the burden of the Collection on respondents, including the use of automated collection techniques or other forms of information technology.

In response to your comments, we may revise this ICR or decide not to seek an extension of approval for the Collection. We will consider all comments and material received during the comment period.

We encourage you to respond to this request by submitting comments and related materials. Comments must contain the OMB Control Number of the ICR and the docket number of this request, USCG–2024–0239, and must be received by June 3, 2024.

Submitting Comments

We encourage you to submit comments through the Federal eRulemaking Portal at <https://www.regulations.gov>. If your material cannot be submitted using <https://www.regulations.gov>, contact the person in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions. Documents mentioned in this notice, and all public comments, are in our online docket at <https://www.regulations.gov> and can be viewed by following that website's instructions. Additionally, if you go to the online docket and sign up for email alerts, you will be notified when comments are posted.

We accept anonymous comments. All comments received will be posted without change to <https://www.regulations.gov> and will include any personal information you have provided. For more about privacy and submissions in response to this document, see DHS's eRulemaking System of Records notice (85 FR 14226, March 11, 2020).

Title: Unauthorized Entry into Cuban Territorial Waters.

OMB Control Number: 1625-0106.

Summary: The Coast Guard, pursuant to Presidential proclamation and order of the Secretary of Homeland Security, is requiring U.S. vessels, and vessels without nationality, less than 100 meters, located within the internal waters or the 12 nautical mile territorial sea of the United States, that thereafter enter Cuban territorial waters, to apply for and receive a Coast Guard permit.

Need: The information is collected to regulate departure from U.S. territorial waters of U.S. vessels, and vessels without nationality, and entry thereafter into Cuban territorial waters. The need to regulate this vessel traffic supports ongoing efforts to enforce the Cuban embargo, which is designed to bring about an end to the current government and a peaceful transition to democracy. Accordingly, only applicants that demonstrate prior U.S. government approval for exports to and transactions with Cuba will be issued a Coast Guard permit.

The permit regulation requires that applicants hold United States Department of Commerce, Bureau of Industry and Security (BIS) and U.S. Department of Treasury the Office of Foreign Assets Control (OFAC) licenses that permit exports to and transactions with Cuba. The USCG permit process thus allows the agency to collect information from applicants about their status vis-à-vis BIS and OFAC licenses and monitor compliance with BIS and OFAC regulations. These two agencies administer statutes and regulations that proscribe exports to (BIS) and transactions with (OFAC) Cuba. Accordingly, in order to assist BIS and OFAC in the enforcement of these license requirements, as directed by the President and the Secretary of Homeland Security, the Coast Guard is requiring certain U.S. vessels, and vessels without nationality, to demonstrate that they hold these

licenses before they depart for Cuban waters.

Forms: CG-3300, Application for Permit to Enter Cuban Territorial Seas.

Respondents: Owners and operators of vessels.

Frequency: On occasion.

Hour Burden Estimate: The estimated burden remains around 5 hours per year.

Authority: The Paperwork Reduction Act of 1995; 44 U.S.C. chapter 35, as amended.

Dated: March 29, 2024.

Kathleen Claffie,

Chief, Office of Privacy Management, U.S. Coast Guard.

[FR Doc. 2024-07126 Filed 4-3-24; 8:45 am]

BILLING CODE 9110-04-P

DEPARTMENT OF HOMELAND SECURITY

U.S. Customs and Border Protection

Quarterly IRS Interest Rates Used in Calculating Interest on Overdue Accounts and Refunds of Customs Duties

AGENCY: U.S. Customs and Border Protection, Department of Homeland Security.

ACTION: General notice.

SUMMARY: This notice advises the public that the quarterly Internal Revenue Service interest rates used to calculate interest on overdue accounts (underpayments) and refunds (overpayments) of customs duties will remain the same from the previous quarter. For the calendar quarter beginning April 1, 2024, the interest rates for underpayments will be 8 percent for both corporations and non-corporations. The interest rate for overpayments will be 8 percent for non-corporations and 7 percent for corporations. This notice is published for the convenience of the importing public and U.S. Customs and Border Protection personnel.

DATES: The rates announced in this notice are applicable as of April 1, 2024.

FOR FURTHER INFORMATION CONTACT: Bruce Ingalls, Revenue Division, Collection Refunds & Analysis Branch, 6650 Telecom Drive, Suite #100, Indianapolis, Indiana 46278; telephone (317) 298-1107.

SUPPLEMENTARY INFORMATION:

Background

Pursuant to 19 U.S.C. 1505 and Treasury Decision 85-93, published in the **Federal Register** on May 29, 1985 (50 FR 21832), the interest rate paid on applicable overpayments or underpayments of customs duties must be in accordance with the Internal Revenue Code rate established under 26 U.S.C. 6621 and 6622. Section 6621 provides different interest rates applicable to overpayments: one for corporations and one for non-corporations.

The interest rates are based on the Federal short-term rate and determined by the Internal Revenue Service (IRS) on behalf of the Secretary of the Treasury on a quarterly basis. The rates effective for a quarter are determined during the first-month period of the previous quarter.

In Revenue Ruling 2024-6, the IRS determined the rates of interest for the calendar quarter beginning April 1, 2024, and ending on June 30, 2024. The interest rate paid to the Treasury for underpayments will be the Federal short-term rate (5%) plus three percentage points (3%) for a total of eight percent (8%) for both corporations and non-corporations. For overpayments made by non-corporations, the rate is the Federal short-term rate (5%) plus three percentage points (3%) for a total of eight percent (8%). For corporate overpayments, the rate is the Federal short-term rate (5%) plus two percentage points (2%) for a total of seven percent (7%). These interest rates used to calculate interest on overdue accounts (underpayments) and refunds (overpayments) of customs duties remain the same from the previous quarter. These interest rates are subject to change for the calendar quarter beginning July 1, 2024, and ending on September 30, 2024.

For the convenience of the importing public and U.S. Customs and Border Protection personnel, the following list of IRS interest rates used, covering the period from July of 1974 to date, to calculate interest on overdue accounts and refunds of customs duties, is published in summary format.

Beginning date	Ending date	Underpayments (percent)	Overpayments (percent)	Corporate overpayments (eff. 1-1-99) (percent)
070174	063075	6	6
070175	013176	9	9

Beginning date	Ending date	Underpayments (percent)	Overpayments (percent)	Corporate overpayments (eff. 1–1–99) (percent)
020176	013178	7	7	
020178	013180	6	6	
020180	013182	12	12	
020182	123182	20	20	
010183	063083	16	16	
070183	123184	11	11	
010185	063085	13	13	
070185	123185	11	11	
010186	063086	10	10	
070186	123186	9	9	
010187	093087	9	8	
100187	123187	10	9	
010188	033188	11	10	
040188	093088	10	9	
100188	033189	11	10	
040189	093089	12	11	
100189	033191	11	10	
040191	123191	10	9	
010192	033192	9	8	
040192	093092	8	7	
100192	063094	7	6	
070194	093094	8	7	
100194	033195	9	8	
040195	063095	10	9	
070195	033196	9	8	
040196	063096	8	7	
070196	033198	9	8	
040198	123198	8	7	
010199	033199	7	7	6
040199	033100	8	8	7
040100	033101	9	9	8
040101	063001	8	8	7
070101	123101	7	7	6
010102	123102	6	6	5
010103	093003	5	5	4
100103	033104	4	4	3
040104	063004	5	5	4
070104	093004	4	4	3
100104	033105	5	5	4
040105	093005	6	6	5
100105	063006	7	7	6
070106	123107	8	8	7
010108	033108	7	7	6
040108	063008	6	6	5
070108	093008	5	5	4
100108	123108	6	6	5
010109	033109	5	5	4
040109	123110	4	4	3
010111	033111	3	3	2
040111	093011	4	4	3
100111	033116	3	3	2
040116	033118	4	4	3
040118	123118	5	5	4
010119	063019	6	6	5
070119	063020	5	5	4
070120	033122	3	3	2
040122	063022	4	4	3
070122	093022	5	5	4
100122	123122	6	6	5
010123	093023	7	7	6
100123	063024	8	8	7

Dated: March 28, 2024.

Crinley S. Hoover,
*Acting Chief Financial Officer, U.S. Customs
 and Border Protection.*

[FR Doc. 2024–07133 Filed 4–3–24; 8:45 am]

BILLING CODE 9111–14–P

DEPARTMENT OF THE INTERIOR**Bureau of Indian Affairs**

[245A2100DD/AAK001030/
AOA501010.999900]

Rate Adjustments for Indian Irrigation Projects; Correction

AGENCY: Bureau of Indian Affairs, Interior.

ACTION: Notice; correction.

SUMMARY: The Bureau of Indian Affairs (BIA) published a document in the *Federal Register* of February 8, 2024, concerning BIA's request for comments on proposed assessment rates to recover the costs to administer, operate, maintain, and rehabilitate its irrigation projects. The document contained an incorrect date.

FOR FURTHER INFORMATION CONTACT: Leslie Underwood, Program Specialist, Division of Water and Power, Office of Trust Services, (406) 657-5985.

SUPPLEMENTARY INFORMATION:*Correction*

In the *Federal Register* of February 8, 2024, FR Doc. 2024-02596, on page 8708, in the second column, correct the answer to the question "When will you put the rate adjustments into effect?" to read:

We will put the rate adjustments into effect for CY 2025.

Dated: March 29, 2024.

George Patton,

Regulatory Documentation Specialist.

[FR Doc. 2024-07157 Filed 4-3-24; 8:45 am]

BILLING CODE 4337-15-P

DEPARTMENT OF THE INTERIOR

[242D0102DM, DS6CS00000,
DLSN00000.000000, DX6CS25; OMB Control
No. 1090-0013]

Agency Information Collection Activities; Submission to the Office of Management and Budget for Review and Approval; Watercraft Inspection and Decontamination Regional Data-Sharing for Trailered Boats

AGENCY: Department of the Interior.

ACTION: Notice of information collection; request for comment.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995, we, the Department of the Interior (Interior) are proposing to renew an information collection with revisions.

DATES: Interested persons are invited to submit comments on or before June 3, 2024.

ADDRESSES: Send your comments on this information collection request (ICR) by mail to Mr. Jeffrey Parrillo, Departmental Information Collection Clearance Officer, 1849 C Street NW, Washington, DC 20240; or by email to DOI-PRA@ios.doi.gov. Please reference OMB Control Number 1090-0013 in the subject line of your comments.

FOR FURTHER INFORMATION CONTACT: To request additional information about this ICR, contact Heidi McMaster, Natural Resources Specialist, by email at hcmaster@usbr.gov, or by telephone at (208) 860-9649. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States.

SUPPLEMENTARY INFORMATION: In accordance with the Paperwork Reduction Act of 1995 (PRA, 44 U.S.C. 3501 *et seq.*) and 5 CFR 1320.8(d)(1), all information collections require approval under the PRA. We may not conduct or sponsor and you are not required to respond to a collection of information unless it displays a currently valid OMB control number.

As part of our continuing effort to reduce paperwork and respondent burdens, we invite the public and other Federal agencies to comment on new, proposed, revised, and continuing collections of information. This helps us assess the impact of our information collection requirements and minimize the public's reporting burden. It also helps the public understand our information collection requirements and provide the requested data in the desired format.

We are especially interested in public comment addressing the following:

- (1) Whether or not the collection of information is necessary for the proper performance of the functions of the agency, including whether or not the information will have practical utility;
- (2) The accuracy of our estimate of the burden for this collection of information, including the validity of the methodology and assumptions used;
- (3) Ways to enhance the quality, utility, and clarity of the information to be collected; and
- (4) How might the agency minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological

collection techniques or other forms of information technology, *e.g.*, permitting electronic submission of response.

Comments that you submit in response to this notice are a matter of public record. We will include or summarize each comment in our request to OMB to approve this ICR. Before including your address, phone number, email address, or other personal identifying information in your comment, you should be aware that your entire comment—including your personal identifying information—may be made publicly available at any time. While you can ask us in your comment to withhold your personal identifying information from public review, we cannot guarantee that we will be able to do so.

Abstract: Interior is authorized by the Lacey Act (18 U.S.C. 42, 16 U.S.C. 3371-3378 *et seq.*), the Fish and Wildlife Coordination Act (U.S.C. 661 *et seq.*, as amended by John D. Dingell, Jr. Conservation, Management, and Recreation Act, Title 25 U.S.C. 3701, *et seq.* sec. 7001(b)(2), Pub. L. 116-9) and the Federal Land Policy and Management Act of 1976, as amended, 43 U.S.C. 1701, *et seq.*, to collect this information. Interior is requesting approval to collect information from boaters entering or exiting water areas managed by various bureaus under Interior. The data will help document the presence and evaluate any risks associated with the unintentional introduction of quagga/zebra mussels and other aquatic invasive species in waters managed by the various bureaus under Interior. Collection of this information is required for all watercrafts entering and exiting waters managed by the various bureaus under Interior that have an active watercraft inspection and decontamination program.

The Regional Watercraft Inspection Decontamination Data Sharing System (Regional Database) was developed by the State of Colorado and is currently being utilized by numerous entities within the Western Regional Panel on Aquatic Nuisance Species (WRP). The National Park Service (NPS), U.S. Fish and Wildlife Service, Bureau of Reclamation, and Bureau of Land Management are part of the WRP and the regional network of state and federal agencies working to prevent the spread of quagga/zebra mussels and other aquatic invasive species (AIS) in the western U.S. The success of this multi-agency effort relies in part upon timely availability of accurate information related to trailered boats at watercraft inspection/decontamination (WID) stations. The Regional Database makes

this information available to staff at WID stations, allowing them to assess risk associated with quagga/zebra mussels and other AIS on trailered boats. States have asked Federal partner agencies to use the Regional Database at their sites with WID programs.

Using the Regional Database requires that WID personnel ask boaters four questions and enter the responses via an app on a smartphone or tablet. Two of the four questions vary depending on whether a boater is entering or exiting the waterbody; the other two questions are the same for entering or exiting boaters:

Upon Entering:

1. Has the boat been out of the state in the last 30 days?
2. Where will the boat be launched next?

Upon Entering or Exiting:

1. What compartments or containers on the boat, including ballast tanks, hold water?
2. Does the boater have any live aquatic bait?

Proposed Revision

We would like to revise the information collection to include watercraft owner or boat hauler/transporter zip code. We are also changing the response time from 4 minutes to 3 minutes.

Title of Collection: Watercraft Inspection Decontamination Regional Data-Sharing for Trailered Boats.

OMB Control Number: 1090-0013.

Form Number: None.

Type of Review: Revision of already approved information collection.

Respondents/Affected Public: Individuals/household; private sector; State, local, and Tribal governments.

Total Estimated Number of Annual Respondents: 416,376.

Total Estimated Number of Annual Responses: 416,376.

Estimated Completion Time per Response: 3 minutes.

Total Estimated Number of Annual Burden Hours: 20,816 hours.

Respondent's Obligation: Mandatory.

Frequency of Collection: On occasion. (Upon entry, exit, or both).

Total Estimated Annual Nonhour Burden Cost: None.

An agency may not conduct or sponsor and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number.

The authority for this action is the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*).

Jeffrey Parrillo,

Departmental Information Collection Clearance Officer.

[FR Doc. 2024-07155 Filed 4-3-24; 8:45 am]

BILLING CODE 4334-63-P

DEPARTMENT OF THE INTERIOR

Office of the Secretary

[245D0102DM, DS600000, DLSN00000.000000, DX6CS25; OMB Control Number 1040-0001]

Agency Information Collection Activities; DOI Programmatic Clearance for Customer Satisfaction Surveys

AGENCY: Office of the Secretary, Interior.

ACTION: Notice of information collection; request for comment.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995, the Office of the Secretary are proposing to renew an information collection, without change.

DATES: Interested persons are invited to submit comments on or before June 3, 2024.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent to the Departmental Information Collection Clearance Officer (ICCO), 1849 C Street NW, Washington, DC 20240; or by email to PRA@ios.doi.gov. Please reference OMB Control Number 1040-0001 in the subject line of your comments.

FOR FURTHER INFORMATION CONTACT: To request additional information about this ICR, contact Jeffrey Parrillo, Departmental ICCO, 1849 C Street NW, Washington, DC 20240; by telephone at (202) 208-7072, or by email to PRA@ios.doi.gov. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States.

SUPPLEMENTARY INFORMATION: In accordance with the Paperwork Reduction Act (PRA, 44 U.S.C. 3501 *et seq.*) and its implementing regulations at 5 CFR 1320.8(d)(1), all information collections require approval under the PRA. We may not conduct or sponsor and you are not required to respond to a collection of information unless it

displays a currently valid OMB control number.

As part of our continuing effort to reduce paperwork and respondent burdens, we invite the public and other Federal agencies to comment on new, proposed, revised, and continuing collections of information. This helps us assess the impact of our information collection requirements and minimize the public's reporting burden. It also helps the public understand our information collection requirements and provide the requested data in the desired format.

We are especially interested in public comment addressing the following:

- (1) Whether or not the collection of information is necessary for the proper performance of the functions of the agency, including whether or not the information will have practical utility;
- (2) The accuracy of our estimate of the burden for this collection of information, including the validity of the methodology and assumptions used;
- (3) Ways to enhance the quality, utility, and clarity of the information to be collected; and
- (4) How might the agency minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.*, permitting electronic submission of response.

Comments that you submit in response to this notice are a matter of public record. We will include or summarize each comment in our request to OMB to approve this ICR. Before including your address, phone number, email address, or other personal identifying information in your comment, you should be aware that your entire comment—including your personal identifying information—may be made publicly available at any time. While you can ask us in your comment to withhold your personal identifying information from public review, we cannot guarantee that we will be able to do so.

Abstract: The Government Performance and Results Act of 1993 (GPRA) (Pub. L. 103-62) requires agencies to “improve Federal program effectiveness and public accountability by promoting a new focus on results, service quality, and customer satisfaction.” To fulfill this responsibility, Department of the Interior (DOI, Interior) bureaus and offices must collect data from their respective user groups to better understand the needs and desires of the public and to respond accordingly.

Executive Order 12862 “Setting Customer Service Standards” also requires all executive departments to “survey customers to determine . . . their level of satisfaction with existing services.” We use customer satisfaction surveys to help us fulfill our responsibilities to provide excellence in government by proactively consulting with those we serve. This programmatic clearance provides an expedited approval process for DOI bureaus and offices to conduct customer research through external surveys such as questionnaires and comment cards.

The proposed renewal covers all of the organizational units and bureaus in DOI. Information obtained from customers by bureaus and offices will be provided voluntarily. No one survey will cover all the topic areas; rather, these topic areas serve as a guide within which the bureaus and offices will develop questions. Questions may be asked in languages other than English (e.g., Spanish) where appropriate. Topic areas include:

(1) Delivery, quality, and value of products, information, and services. Respondents may be asked for feedback regarding the following attributes of the information, service, and products provided:

- (a) Timeliness.
- (b) Consistency.
- (c) Accuracy.
- (d) Ease of Use and Usefulness.
- (e) Ease of Information Access.
- (f) Helpfulness.
- (g) Quality.
- (h) Value for fee paid for information/product/service.

(2) Management practices. This area covers questions relating to how well customers are aware of or satisfied with DOI management practices and processes, what improvements they might make to specific processes, and whether or not they feel specific issues were addressed and reconciled in a timely, courteous, and responsive manner.

(3) Mission management. We will ask customers to provide information of their existing knowledge, agreement, or satisfaction related to DOI’s ability to protect, conserve, provide access to, provide scientific data about, and preserve natural, cultural, and recreational resources that we manage, and how well we are carrying out our trust responsibilities to American Indians.

(4) Rules, regulations, policies. This area focuses on obtaining feedback from customers regarding fairness, adequacy, and consistency in enforcing rules, regulations, and policies for which DOI is responsible. It will also help us

understand public awareness of rules and regulations and whether or not they are explained in a clear and understandable manner.

(5) Interactions with DOI Personnel and Contractors. Questions will range from timeliness and quality of interactions to skill level of staff providing the assistance, as well as their courtesy and responsiveness during the interaction.

(6) General demographics. Some general demographics may be gathered to augment satisfaction questions so that we can better understand the customer and improve how we serve that customer. We may ask customers how many times they have used a service, visitation logistics including timing, distance traveled, and costs, as well as general characteristics (e.g., race, age, residency, etc.) about themselves and their group.

(7) Experience and perceptions. This topic focuses on gathering specific details about the DOI experiences including logistics and planning, motivation for participating, and activities, as well as perceptions about the values, interactions, and activities. Similar to demographics, this information may augment satisfaction questions so that we can better understand the customer and improve how we serve that customer.

All requests to collect information under the auspices of this proposed renewal will be carefully evaluated to ensure consistency with the intent, requirements, and boundaries of this programmatic clearance. Interior’s Office of Policy Analysis will conduct an administrative and technical review of each specific request in order to ensure statistical validity and soundness. All information collections are required to be designed and deployed based upon acceptable statistical practices and sampling methodologies, and procedures that account for and minimize non-response bias, in order to obtain consistent, valid data and statistics that are representative of the target populations.

Title of Collection: DOI Programmatic Clearance for Customer Satisfaction Surveys.

OMB Control Number: 1040–0001.

Form Number: DI–4010.

Type of Review: Extension of a currently approved collection.

Respondents/Affected Public: DOI customers, stakeholders, and partners. We define customers as anyone who uses, or could potentially use, DOI resources, products, or services. This includes past, current, and potential customers (e.g., the American public, representatives of the private sector,

academia, and other government agencies). We define stakeholders to mean groups or individuals who have an expressed interest in and who seek to influence the present and future state of DOI’s resources, products, and services. We define partners as those groups, individuals, and agencies who are formally engaged in helping DOI accomplish its mission.

Total Estimated Number of Annual Respondents: 65,000.

Total Estimated Number of Annual Responses: 65,000.

Average Completion Time per Response: 10 minutes.

Total Estimated Number of Annual Burden Hours: 10,833.

Respondent’s Obligation: Voluntary.

Frequency of Collection: On occasion.

Total Estimated Annual Nonhour Burden Cost: None.

An agency may not conduct or sponsor and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number.

The authority for this action is the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*).

Jeffrey Parrillo,

Departmental Information Collection Clearance Officer.

[FR Doc. 2024–07153 Filed 4–3–24; 8:45 am]

BILLING CODE 4334–63–P

DEPARTMENT OF THE INTERIOR

Bureau of Land Management

[BLM_CA_FRN_MO4500170079]

Notice of Public Meeting of the Central California Resource Advisory Council

AGENCY: Bureau of Land Management, Interior.

ACTION: Notice of public meeting.

SUMMARY: In accordance with the Federal Land Policy and Management Act and the Federal Advisory Committee Act, the U.S. Department of the Interior, Bureau of Land Management’s (BLM) Central California Resource Advisory Council (RAC) will meet as follows.

DATES: A field tour will be held on May 8, 2024, from 12:30 p.m. to 5 p.m. Pacific Time (PT). The Central California RAC will hold a public meeting on May 9, 2024, from 8:30 a.m. to 4 p.m. PT, with a virtual participation option. Written public comments will be accepted prior to the meeting, and a public comment opportunity will begin at 3:30 p.m. PT on the business meeting day. If weather or circumstances arise

that prohibit an on-site meeting, the field tour will be cancelled, and the business meeting will be held in an all-virtual format via Zoom, or the meeting will be cancelled. The meeting and field tour are open to the public.

ADDRESSES: The final agenda for the public meeting will be posted on the BLM's web page two weeks in advance of the meeting at <https://go.usa.gov/xH9ya>. The field tour details, a virtual meeting link, and participation instructions will be made available to the public via BLM news release and the RAC's web page at least two weeks prior to the meeting. The May 8, 2024, field tour will be to the Berryessa Snow Mountain National Monument. The field tour will commence and conclude at Seke Hills Olive Mill, 19326 Country Road 78, Brooks, CA 95606. The May 9, 2024, meeting will be held at the Cache Creek Casino Resort, 14455 Highway 16, Brooks, CA 95606.

Written comments pertaining to the meeting can be sent to the BLM Central California District Office, 5152 Hillsdale Circle, El Dorado Hills, CA 95762, Attention: RAC meeting comments.

FOR FURTHER INFORMATION CONTACT: Public Affairs Officer Philip Oviatt, email: poviatt@blm.gov, or telephone: (661) 432-4252. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services. Individuals outside the United States should use the relay services offered within their country to make international calls to the point-of-contact in the United States.

SUPPLEMENTARY INFORMATION: Topics for the RAC meeting are as follows: On May 8, 2024, the RAC will tour the Berryessa Snow Mountain National Monument to view a variety of resources, visitor uses, and management activities. To attend the field tour, please RSVP by Friday, May 3, to the individual listed in the **FOR FURTHER INFORMATION** section of this notice. On May 9, 2024, the RAC will be briefed on the management of the Berryessa Snow Mountain National Monument and identify opportunities to engage in the Monument planning process. The RAC will also receive presentations and make recommendations on fee proposals from the U.S. Department of Agriculture Forest Service for multiple sites located in the Los Padres National Forest, the Sierra National Forest, and the Tahoe National Forest. In addition, the RAC will schedule additional meeting dates for 2024-2025.

The meeting and field tour are open to the public. The formal RAC meeting will have time allocated for public comments. Depending on the number of persons wishing to speak and the time available, the amount of time for oral comments may be limited. Written public comments may be sent to the BLM Central California District Office listed in the **ADDRESSES** section of this notice. All comments received will be provided to the RAC. Before including your address, phone number, email address, or other personal identifying information in your comment, you should be aware that your entire comment—including your personal identifying information—may be made publicly available at any time. While you can ask us in your comment to withhold your personal identifying information from public review, we cannot guarantee that we will be able to do so.

Members of the public wishing to participate in the field tour must provide their own transportation and meals.

Meeting Accessibility/Special Accommodations: For sign language interpreter services, assistive listening devices, or other reasonable accommodations, please contact the BLM (see **FOR FURTHER INFORMATION CONTACT**) at least seven business days before the meeting to ensure there is sufficient time to process the request. The Department of the Interior manages accommodation requests on a case-by-case basis.

Detailed minutes for the RAC meetings will be maintained in the BLM Central California District Office. Minutes will also be posted to the BLM Central California RAC web page.

(Authority: 43 CFR 1784.4-2)

Erica St. Michel,

Deputy State Director, Communications.

[FR Doc. 2024-07168 Filed 4-3-24; 8:45 am]

BILLING CODE 4331-15-P

DEPARTMENT OF THE INTERIOR

Bureau of Land Management

[BLM_AK_FRN_MO4500172131; F-14837-G2]

Alaska Native Claims Selection

AGENCY: Bureau of Land Management, Interior.

ACTION: Notice of decision approving lands for conveyance.

SUMMARY: The Bureau of Land Management (BLM) hereby provides constructive notice that it will issue an

appealable decision approving conveyance of the surface estate in certain lands to Beaver Kwit'chin Corporation for the Native village of Beaver, pursuant to the Alaska Native Claims Settlement Act of 1971 (ANCSA). The subsurface estate in the same lands will be conveyed to Doyon, Limited, when the surface estate is conveyed to Beaver Kwit'chin Corporation.

DATES: Any party claiming a property interest in the lands affected by the decision may appeal the decision in accordance with the requirements of 43 CFR part 4 within the time limits set out in the **SUPPLEMENTARY INFORMATION** section.

ADDRESSES: You may obtain a copy of the decision from the Bureau of Land Management, Alaska State Office, 222 West Seventh Avenue, #13, Anchorage, AK 99513-7504.

FOR FURTHER INFORMATION CONTACT: Matthew Colburn, Land Law Examiner, Adjudication Section, BLM Alaska State Office, 907-271-5067 or mcolburn@blm.gov. Individuals in the United States who are deaf, deafblind, hard of hearing, or have a speech disability may dial 711 (TTY, TDD, or TeleBraille) to access telecommunications relay services. Individuals outside the United States should use the relay services offered within their country to make international calls to the point of contact in the United States.

SUPPLEMENTARY INFORMATION: As required by 43 CFR 2650.7(d), notice is hereby given that the BLM will issue an appealable decision to Beaver Kwit'chin Corporation. The decision approves conveyance of the surface estate in certain lands pursuant to ANCSA (43 U.S.C. 1601, *et seq.*), as amended. As provided by ANCSA, the subsurface estate in the same lands will be conveyed to Doyon, Limited, when the surface estate is conveyed to Beaver Kwit'chin Corporation. The lands are located in the vicinity of Beaver, Alaska, and are described as:

Fairbanks Meridian, Alaska

T. 16 N., R. 1 E.,
Secs. 21, 22, and 23;
Secs. 25 to 28, inclusive;
Secs. 33, 34, and 35.
Containing 4,920.11 acres.

The decision addresses public access easements, if any, to be reserved to the United States pursuant to sec. 17(b) of ANCSA (43 U.S.C. 1616(b)), in the lands described above.

The BLM will also publish notice of the decision once a week for four consecutive weeks in the Fairbanks Daily News-Miner newspaper.

Any party claiming a property interest in the lands affected by the decision may appeal the decision in accordance with the requirements of 43 CFR part 4 within the following time limits:

1. Unknown parties, parties unable to be located after reasonable efforts have been expended to locate, parties who fail or refuse to sign their return receipt, and parties who receive a copy of the decision by regular mail which is not certified, return receipt requested, shall have until May 6, 2024 to file an appeal.

2. Parties receiving service of the decision by certified mail shall have 30 days from the date of receipt to file an appeal.

Parties who do not file an appeal in accordance with the requirements of 43 CFR part 4 shall be deemed to have waived their rights. Notices of appeal transmitted by facsimile will not be accepted as timely filed.

Matthew A. Colburn,

Land Law Examiner, Adjudication Section.

[FR Doc. 2024-07171 Filed 4-3-24; 8:45 am]

BILLING CODE 4331-10-P

INTERNATIONAL TRADE COMMISSION

[Investigation Nos. 701-TA-598 and 731-TA-1408 and 1410 (Review)]

Rubber Bands From China and Thailand; Notice of Termination of Five-Year Reviews

AGENCY: International Trade Commission.

ACTION: Notice.

SUMMARY: The Commission instituted the subject five-year reviews on January 2, 2024, to determine whether revocation of the countervailing duty order on rubber bands from China and the antidumping duty orders on rubber bands from China and Thailand would be likely to lead to continuation or recurrence of material injury. On March 21, 2024, the Department of Commerce published notice in the **Federal Register** that it was revoking the orders because no domestic interested party filed a timely notice of intent to participate. The effective date of the revocation of the antidumping and countervailing duty orders on imports of rubber bands from China is February 19, 2024. The effective date of the revocation of the antidumping duty order on imports of rubber bands from Thailand is April 26, 2024. Accordingly, the subject reviews are terminated.

DATES: *Effective dates:*

February 19, 2024: Rubber Bands from China (Investigation Nos. 701-TA-598 and 731-TA-1408 (First Review))
April 26, 2024: Rubber Bands from Thailand (Investigation No. 731-TA-1410 (First Review))

FOR FURTHER INFORMATION CONTACT: Alec Resch (202-708-1448), Office of Investigations, U.S. International Trade Commission, 500 E Street SW, Washington, DC 20436. Hearing-impaired individuals are advised that information on this matter can be obtained by contacting the Commission's TDD terminal on 202-205-1810. Persons with mobility impairments who will need special assistance in gaining access to the Commission should contact the Office of the Secretary at 202-205-2000. General information concerning the Commission may also be obtained by accessing its internet server (<https://www.usitc.gov>). The public record for these investigations may be viewed on the Commission's electronic docket (EDIS) at <https://edis.usitc.gov>.

Authority: These reviews are being terminated under authority of title VII of the Tariff Act of 1930 and pursuant to section 751(c) of the Tariff Act of 1930 (19 U.S.C. 1675(c)). This notice is published pursuant to section 207.69 of the Commission's rules (19 CFR 207.69).

By order of the Commission.

Issued: April 1, 2024.

Lisa Barton,

Secretary to the Commission.

[FR Doc. 2024-07167 Filed 4-3-24; 8:45 am]

BILLING CODE 7020-02-P

INTERNATIONAL TRADE COMMISSION

[Investigation Nos. 701-TA-706-709 and 731-TA-1667-1672 (Preliminary)]

Melamine From Germany, India, Japan, Netherlands, Qatar, and Trinidad and Tobago; Determinations

On the basis of the record¹ developed in the subject investigations, the United States International Trade Commission ("Commission") determines, pursuant to the Tariff Act of 1930 ("the Act"), that there is a reasonable indication that an industry in the United States is materially injured by reason of imports of melamine from Germany, India, Netherlands, Qatar, and Trinidad and Tobago, provided for in subheading 2933.61.00 of the Harmonized Tariff Schedule of the United States, that are

alleged to be sold in the United States at less than fair value ("LTFV") and alleged to be subsidized by the Governments of Germany, India, Qatar, and Trinidad and Tobago.² The Commission also determines that there is a reasonable indication that an industry in the United States is threatened with material injury by reason of imports of melamine from Japan, provided for in subheading 2933.61.00 of the Harmonized Tariff Schedule of the United States, that are alleged to be sold in the United States at LTFV.³

Commencement of Final Phase Investigations

Pursuant to section 207.18 of the Commission's rules, the Commission also gives notice of the commencement of the final phase of its investigations. The Commission will issue a final phase notice of scheduling, which will be published in the **Federal Register** as provided in § 207.21 of the Commission's rules, upon notice from the U.S. Department of Commerce ("Commerce") of affirmative preliminary determinations in the investigations under §§ 703(b) or 733(b) of the Act, or, if the preliminary determinations are negative, upon notice of affirmative final determinations in those investigations under §§ 705(a) or 735(a) of the Act. Parties that filed entries of appearance in the preliminary phase of the investigations need not enter a separate appearance for the final phase of the investigations. Any other party may file an entry of appearance for the final phase of the investigations after publication of the final phase notice of scheduling. Industrial users, and, if the merchandise under investigation is sold at the retail level, representative consumer organizations have the right to appear as parties in Commission antidumping and countervailing duty investigations. The Secretary will prepare a public service list containing the names and addresses of all persons, or their representatives, who are parties to the investigations. As provided in section 207.20 of the Commission's rules, the Director of the Office of Investigations will circulate draft questionnaires for the final phase of the investigations to parties to the investigations, placing copies on the Commission's Electronic Document Information System (EDIS, <https://edis.usitc.gov>), for comment.

¹ The record is defined in § 207.2(f) of the Commission's Rules of Practice and Procedure (19 CFR 207.2(f)).

² 89 FR 17381 and 89 FR 17413 (March 11, 2024).

³ 89 FR 17413 (March 11, 2024).

Background

On February 14, 2024, Cornerstone Chemical Company, Waggaman, Louisiana, filed petitions with the Commission and Commerce, alleging that an industry in the United States is materially injured or threatened with material injury by reason of subsidized imports of melamine from Germany, India, Qatar, and Trinidad and Tobago and LTFV imports of melamine from Germany, India, Japan, Netherlands, Qatar, and Trinidad and Tobago. Accordingly, effective February 14, 2024, the Commission instituted countervailing duty investigation Nos. 701-TA-706-709 and antidumping duty investigation Nos. 731-TA-1667-1672 (Preliminary).

Notice of the institution of the Commission's investigations and of a public conference to be held in connection therewith was given by posting copies of the notice in the Office of the Secretary, U.S. International Trade Commission, Washington, DC, and by publishing the notice in the **Federal Register** of February 21, 2024 (89 FR 13090). The Commission conducted its conference on March 6, 2024. All persons who requested the opportunity were permitted to participate.

The Commission made these determinations pursuant to §§ 703(a) and 733(a) of the Act (19 U.S.C. 1671b(a) and 1673b(a)). It completed and filed its determinations in these investigations on April 1, 2024. The views of the Commission are contained in USITC Publication 5503 (April 2024), entitled *Melamine from Germany, India, Japan, Netherlands, Qatar, and Trinidad and Tobago: Investigation Nos. 701 TA-706-709 and 731-TA-1667-1672 (Preliminary)*.

By order of the Commission.

Issued: April 1, 2024.

Lisa Barton,

Secretary to the Commission.

[FR Doc. 2024-07181 Filed 4-3-24; 8:45 am]

BILLING CODE 7020-02-P

DEPARTMENT OF JUSTICE

Drug Enforcement Administration

[Docket No. DEA-1350]

Bulk Manufacturer of Controlled Substances Application: Sterling Wisconsin, LLC

AGENCY: Drug Enforcement Administration, Justice.

ACTION: Notice of application.

SUMMARY: Sterling Wisconsin, LLC has applied to be registered as a bulk manufacturer of basic class(es) of controlled substance(s). Refer to **SUPPLEMENTARY INFORMATION** listed below for further drug information.

DATES: Registered bulk manufacturers of the affected basic class(es), and applicants therefore, may submit electronic comments on or objections to the issuance of the proposed registration on or before June 3, 2024. Such persons may also file a written request for a hearing on the application on or before June 3, 2024.

ADDRESSES: The Drug Enforcement Administration requires that all comments be submitted electronically through the Federal eRulemaking Portal, which provides the ability to type short comments directly into the comment field on the web page or attach a file for lengthier comments. Please go to <https://www.regulations.gov> and follow the online instructions at that site for submitting comments. Upon submission of your comment, you will receive a Comment Tracking Number. Please be aware that submitted comments are not instantaneously available for public view on <https://www.regulations.gov>. If you have received a Comment Tracking Number, your comment has been successfully submitted and there is no need to resubmit the same comment.

SUPPLEMENTARY INFORMATION: In accordance with 21 CFR 1301.33(a), this is notice that on February 27, 2024, Sterling Wisconsin, LLC, W130N10497 Washington Drive, Germantown, Wisconsin 53022-4448, applied to be registered as a bulk manufacturer of the following basic class(es) of controlled substance(s):

Controlled substance	Drug code	Schedule
Lysergic Acid Diethylamide.	7315	I
Marihuana Extract	7350	I
Marihuana	7360	I
Tetrahydrocannabinols ..	7370	I
Mescaline	7381	I
5-Methoxy-N-N-Dimethyltryptamine.	7431	I
Psilocybin	7437	I
Oliceridine	9245	II
Thebaine	9333	II
Alfentanil	9737	II

The company plans to bulk manufacture the listed controlled substances for commercial sale to its customers. In reference to drug codes 7350 (Marihuana Extract), 7360 (Marihuana), and 7370 (Tetrahydrocannabinols), the company plans to bulk manufacture these drugs as synthetic. No other activities for these

drug codes are authorized for this registration.

Marsha Ikner,

Acting Deputy Assistant Administrator.

[FR Doc. 2024-07110 Filed 4-3-24; 8:45 am]

BILLING CODE P

DEPARTMENT OF JUSTICE

Drug Enforcement Administration

[Docket No. DEA-1348]

Bulk Manufacturer of Controlled Substances Application: Patheon Pharmaceuticals Inc.

AGENCY: Drug Enforcement Administration, Justice.

ACTION: Notice of application.

SUMMARY: Patheon Pharmaceuticals Inc. has applied to be registered as a bulk manufacturer of basic class(es) of controlled substance(s). Refer to **SUPPLEMENTARY INFORMATION** listed below for further drug information.

DATES: Registered bulk manufacturers of the affected basic class(es), and applicants therefore, may submit electronic comments on or objections to the issuance of the proposed registration on or before June 3, 2024. Such persons may also file a written request for a hearing on the application on or before June 3, 2024.

ADDRESSES: The Drug Enforcement Administration requires that all comments be submitted electronically through the Federal eRulemaking Portal, which provides the ability to type short comments directly into the comment field on the web page or attach a file for lengthier comments. Please go to <https://www.regulations.gov> and follow the online instructions at that site for submitting comments. Upon submission of your comment, you will receive a Comment Tracking Number. Please be aware that submitted comments are not instantaneously available for public view on <https://www.regulations.gov>. If you have received a Comment Tracking Number, your comment has been successfully submitted and there is no need to resubmit the same comment.

SUPPLEMENTARY INFORMATION: In accordance with 21 CFR 1301.33(a), this is notice that on February 28, 2024, Patheon Pharmaceuticals Inc., 2110 East Galbraith Road, Cincinnati, Ohio 45237-1625, applied to be registered as a bulk manufacturer of the following basic class(es) of controlled substance(s):

Controlled substance	Drug code	Schedule
Gamma Hydroxybutyric Acid.	2010	I

The company plans to manufacture the above listed controlled substance as Active Pharmaceutical Ingredient that will be further synthesized into Food and Drug Administration-approved dosage forms. No other activities for this drug code are authorized for this registration.

Marsha L. Ikner,
Acting Deputy Assistant Administrator.
[FR Doc. 2024-07109 Filed 4-3-24; 8:45 am]
BILLING CODE P

DEPARTMENT OF JUSTICE

Drug Enforcement Administration

[Docket No. DEA-1351]

Importer of Controlled Substances Application: Lonza Tampa, LLC

AGENCY: Drug Enforcement Administration, Justice.

ACTION: Notice of application.

SUMMARY: Lonza Tampa, LLC. has applied to be registered as an importer of basic class(es) of controlled substance(s). Refer to **SUPPLEMENTARY INFORMATION** listed below for further drug information.

DATES: Registered bulk manufacturers of the affected basic class(es), and applicants therefore, may submit electronic comments on or objections to the issuance of the proposed registration on or before May 6, 2024. Such persons may also file a written request for a hearing on the application on or before May 6, 2024.

ADDRESSES: The Drug Enforcement Administration requires that all comments be submitted electronically through the Federal eRulemaking Portal, which provides the ability to type short comments directly into the comment field on the web page or attach a file for lengthier comments. Please go to <https://www.regulations.gov> and follow the online instructions at that site for submitting comments. Upon submission of your comment, you will receive a Comment Tracking Number. Please be aware that submitted comments are not instantaneously available for public view on <https://www.regulations.gov>. If you have received a Comment Tracking Number, your comment has been successfully submitted and there is no need to resubmit the same comment. All requests for a hearing must be sent to:

(1) Drug Enforcement Administration, Attn: Hearing Clerk/OALJ, 8701 Morrisette Drive, Springfield, Virginia 22152; and (2) Drug Enforcement Administration, Attn: DEA Federal Register Representative/DPW, 8701 Morrisette Drive, Springfield, Virginia 22152. All requests for a hearing should also be sent to: Drug Enforcement Administration, Attn: Administrator, 8701 Morrisette Drive, Springfield, Virginia 22152.

SUPPLEMENTARY INFORMATION: In accordance with 21 CFR 1301.34(a), this is notice that on March 4, 2024, Lonza Tampa, LLC., 4901 West Grace Street, Tampa, Florida 33607-3805, applied to be registered as an importer of the following basic class(es) of controlled substance(s):

Controlled substance	Drug code	Schedule
Psilocybin	7437	I

The company plans to import drug code 7437 (Psilocybin) as finished dosage units for clinical trials, research, and analytical purposes. No other activities for these drug codes are authorized for this registration.

Approval of permit applications will occur only when the registrant's business activity is consistent with what is authorized under 21 U.S.C. 952(a)(2). Authorization will not extend to the import of Food and Drug Administration-approved or non-approved finished dosage forms for commercial sale.

Marsha Ikner,
Acting Deputy Assistant Administrator.
[FR Doc. 2024-07108 Filed 4-3-24; 8:45 am]
BILLING CODE 4410-09-P

DEPARTMENT OF JUSTICE

Drug Enforcement Administration

[Docket No. DEA-1352]

Bulk Manufacturer of Controlled Substances Application: Benuvia Operations, LLC

AGENCY: Drug Enforcement Administration, Justice.

ACTION: Notice of application.

SUMMARY: Benuvia Operations, LLC has applied to be registered as a bulk manufacturer of basic class(es) of controlled substance(s). Refer to **SUPPLEMENTARY INFORMATION** listed below for further drug information.

DATES: Registered bulk manufacturers of the affected basic class(es), and applicants therefore, may submit

electronic comments on or objections to the issuance of the proposed registration on or before June 3, 2024. Such persons may also file a written request for a hearing on the application on or before June 3, 2024.

ADDRESSES: The Drug Enforcement Administration requires that all comments be submitted electronically through the Federal eRulemaking Portal, which provides the ability to type short comments directly into the comment field on the web page or attach a file for lengthier comments. Please go to <https://www.regulations.gov> and follow the online instructions at that site for submitting comments. Upon submission of your comment, you will receive a Comment Tracking Number. Please be aware that submitted comments are not instantaneously available for public view on <https://www.regulations.gov>. If you have received a Comment Tracking Number, your comment has been successfully submitted and there is no need to resubmit the same comment.

SUPPLEMENTARY INFORMATION: In accordance with 21 CFR 1301.33(a), this is notice that on February 27, 2024, Benuvia Operations, LLC, 3950 North Mays Street, Round Rock, Texas 78665, applied to be registered as a bulk manufacturer of the following basic class(es) of controlled substance(s):

Controlled substance	Drug code	Schedule
Marihuana Extract	7350	I

The company plans to bulk manufacture the listed controlled substance for dosage formulation development. No other activities for these drug codes are authorized for this registration.

Marsha L. Ikner,
Acting Deputy Assistant Administrator.
[FR Doc. 2024-07111 Filed 4-3-24; 8:45 am]
BILLING CODE P

DEPARTMENT OF LABOR

Employee Benefits Security Administration

Technical Correction to PTE 2016-11, Exemption From Certain Prohibited Transaction Restrictions: Northern Trust Corporation (Together With Its Current and Future Affiliates, Northern Trust or the Applicant)

AGENCY: Employee Benefits Security Administration (EBSA), Labor.

ACTION: Notice of Technical Correction.

SUMMARY: This document makes a technical correction to Prohibited Transaction Exemption (PTE) 2016–11 granted to Northern Trust Corporation (D–11875) on October 28, 2016.

DATES:

Issuance Date: This technical correction is issued on April 4, 2024 without further action or notice.

Exemption Date: PTE 2016–11 will remain in effect for the period beginning on the Conviction date (as corrected herein) until the earlier of: (1) the date that is twelve months following the Conviction date; or (2) the effective date of a final agency action made by the Department in connection with an application for long-term exemptive relief for the covered transactions described in PTE 2016–11.

FOR FURTHER INFORMATION CONTACT: Ms. Anna Mpras Vaughan of the Department, telephone (202) 693–8565. (This is not a toll-free number).

SUPPLEMENTARY INFORMATION:

Background

On October 28, 2016, the Department published PTE 2016–11 in the **Federal Register**.¹ PTE 2016–11 is a temporary administrative exemption that permits certain entities (the Northern Trust Qualified Professional Asset Managers (QPAMs)) with specified relationships to Northern Trust Fiduciary Services (Guernsey) Ltd. (NTFS) to continue to rely upon the relief provided by the Department’s QPAM Exemption² for a one-year period, notwithstanding a judgment of conviction against NTFS for aiding and abetting tax fraud.³

The Department granted PTE 2016–11 to protect Covered Plans⁴ from the harm

that could result from the Northern Trust QPAMs’ loss of relief under PTE 84–14 due to the potential conviction of NTFS. Exemptive relief was provided for a period of 12 months from the potential Conviction date to provide the Department with sufficient time to determine whether longer-term relief was appropriate.⁵ PTE 2016–11, as initially granted, defined the term “Conviction” as “the potential judgment of conviction against NTFS for aiding and abetting tax fraud to be entered in France in the District Court of Paris, French Special Prosecutor No. 1120392066, French Investigative Judge No. JIRSIF/11/12.”

In January 2017, the trial court (the Paris District Court) in France acquitted NTFS and all prosecuted parties of the aiding and abetting tax fraud charge, so the exemptive relief provided in PTE 2016–11 was unnecessary. The Paris District Court’s verdict was appealed by the French government to the Paris Court of Appeal, which in March 2018 conducted a retrial and in June 2018 upheld the acquittal of all prosecuted parties on the basis that the offenses were time-barred. The Paris Court of Appeal’s verdict was appealed by the French government to the Court of Cassation, the highest court in France, which in January 2021, quashed the appellate court’s judgment and found that the offenses were not time-barred and there was a legal obligation under French law to declare assets held in certain (but not all) types of trusts.⁶ The Court of Cassation directed a re-trial of all prosecuted parties, including NTFS, and tasked a different panel of the Paris Court of Appeal with ascertaining the nature of the trusts in question. In September–October 2023, the case was tried a third time in front of a different panel of the Paris Court of Appeal. On March 5, 2024, the Paris Court of Appeal issued a judgment of conviction (the 2024 Conviction) against NTFS for aiding and abetting tax fraud. On the

same day, NTFS appealed the verdict to the Court of Cassation.

As a result of the most recent legal proceedings, Northern Trust requests the Department to issue a technical correction to PTE 2016–11 to change the definition of the term “Conviction” in PTE 2016–11 by replacing references to the “District Court of Paris” with references to the “Paris Court of Appeal.” Northern Trust represents that all other identifying information, including the identity of the case and the underlying facts, remain the same.

Before the 2024 Conviction, a separate defendant in the case against Northern Trust, Royal Bank of Canada, requested and received a technical correction to PTE 2016–10.⁷ Northern Trust requested the Department to make the same technical correction to PTE 2016–11 that it made to PTE 2016–10, because PTE 2016–11 also references the “District Court of Paris” case rather than the Paris Court of Appeal case.

As noted above, PTE 2016–11 was granted in order to protect Covered Plans from harm if Northern Trust were convicted for the crime described in that exemption. PTE 2016–11 would have provided 12 months of exemptive relief to Northern Trust in order to afford the Department sufficient time to evaluate whether a longer-term exemption would be in the interest of, and protective of the rights of, Covered Plans and their participants and beneficiaries. This same harm would arise now that NTFS is convicted for the same crime, pursuant to the 2024 Conviction. Therefore, to ensure that Covered Plans are protected from any harm arising from the Conviction while the Department evaluates whether longer-term relief is appropriate, the Department is correcting the definition of “Conviction” in PTE 2016–11 to refer to “the judgment of conviction against NTFS for aiding and abetting tax fraud entered in France in the Court of Appeal, French Special Prosecutor No. 1120392066, French Investigative Judge No. JIRSIF/11/12 or another court of competent jurisdiction.” PTE 2016–11, as corrected, will be effective for a period of 12 months from the date of such Conviction.

The Applicant represents to the Department that, to the best of Northern Trust’s knowledge, there have been no material changes since February 29, 2016, the date of submission of Northern Trust’s exemption application

¹ 81 FR 75150 (October 28, 2016).

² PTE 84–14, 49 FR 9494 (March 13, 1984), as corrected at 50 FR 41430 (October 10, 1985), as amended at 70 FR 49305 (August 23, 2005) and as amended at 75 FR 38837 (July 6, 2010), hereinafter referred to as PTE 84–14 or the QPAM Exemption.

³ Section I(g) of PTE 84–14 prevents an entity that may otherwise meet the definition of a QPAM from utilizing the exemptive relief provided by PTE 84–14 for itself and its client plans, if that entity or an “affiliate” thereof, or any owner, direct or indirect, of a five percent or more interest in the QPAM has within 10 years immediately preceding the transaction, been either convicted or released from imprisonment, whichever is later, as a result of criminal activity described in that section.

⁴ A “Covered Plan” is a plan subject to Part 4 of Title 1 of ERISA (“ERISA-covered plan”) or a plan subject to Section 4975 of the Code (“IRA”), with respect to which a Northern Trust QPAM relies on PTE 84–14, or with respect to which a Northern Trust QPAM (or any Northern Trust affiliate) has expressly represented that the manager qualifies as a QPAM or relies on the QPAM class exemption. A Covered Plan does not include an ERISA-covered Plan or IRA to the extent the Northern Trust QPAM has expressly disclaimed reliance on QPAM status or PTE 84–14 in entering into its contract, arrangement, or agreement with the ERISA-covered plan or IRA.

⁵ Northern Trust’s exemption request (D–11875) is available by contacting EBSA’s Public Disclosure Room at (202) 693–8673.

⁶ The Applicant states that a key issue in this case was whether trust assets were required to be declared as part of an inheritance tax filing. The Court of Cassation held that the legal requirement to declare trust assets as a part of an inheritance applies to trusts where the settlor had not divested of the trust assets during their lifetime. The Paris Court of Appeal analyzed the features and operations of the applicable trusts to determine whether Mr. Wildenstein had effectively divested himself of the trusts’ assets in connection with its March 5, 2024 decision. The Applicant states that the Paris Court of Appeal concluded that Mr. Wildenstein had not effectively divested himself of trust assets.

⁷ See PTE 2016–10, 81 FR 75147 (October 28, 2016). The Department issued a technical correction on December 11, 2023 at 88 FR 85931 that corrected the definition of “Conviction” in PTE 2016–10 to correct the name of the court in France hearing the case as well as the date of conviction.

that serves as the record upon which PTE 2016–11 was proposed and granted, that are relevant to that application or the technical corrections set forth herein, other than changes in Northern Trust's numbers of clients and assets managed. In addition, the Applicant represents that Northern Trust is and has been subject to a variety of legal proceedings, including civil claims and lawsuits, regulatory examinations, investigations, audits, and requests for information by various governmental regulatory agencies and law enforcement authorities in various jurisdictions. To the best of its knowledge at this time, however, Northern Trust does not believe that the outcome of any current investigation would cause the exemption to be unavailable. Moreover, the Applicant represents that no affiliate of Northern Trust has been convicted of any crime described in section I(g) of the QPAM Exemption and, to the best of Northern Trust's knowledge, neither Northern Trust nor any affiliate has entered into a deferred prosecution agreement (DPA) or non-prosecution agreement (NPA) since February 29, 2016.

The Department notes that it is making this technical correction based upon Northern Trust's certified representation that since February 29, 2016: (1) there have in fact been no material changes other than those changes noted above; (2) no affiliate of Northern Trust has been convicted of any crime described in section I(g) of the QPAM Exemption, other than the conviction covered under PTE 2016–11 as corrected herein; (3) neither Northern Trust nor any of its affiliates have entered into a DPA or NPA; and (4) to the best of its knowledge at this time, Northern Trust does not believe that the outcome of any current investigation by any of the various governmental regulatory agencies and law enforcement authorities in various jurisdictions would cause the exemption to be unavailable. If, at any time, Northern Trust discovers that any of these representations are no longer true, Northern Trust must immediately contact the Department and separately submit a written statement that provides the Department with the complete details on the circumstances discovered that led any representations to become untrue.

The Department is not taking a position on whether the outcome of any proceedings will cause the exemption to be unavailable and also notes that the availability of PTE 2016–11 is conditioned upon Northern Trust's compliance with all of the conditions included therein, including the

condition that expressly states: "During the effective period of this temporary exemption, Northern Trust: (1) Immediately discloses to the Department any DPA or NPA that Northern Trust enters into with the U.S. Department of Justice, to the extent such DPA or NPA involves conduct described in Section I(g) of PTE 84–14 or section 411 of ERISA." As noted in the preceding paragraph, if Northern Trust discovers that Northern Trust or any of its affiliates have entered into a DPA or NPA at any time on or after February 29, 2016, Northern Trust must inform the Department promptly upon Northern Trust or its affiliates' discovery of such fact.

Furthermore, if Northern Trust later submits an exemption application requesting longer term exemptive relief from Section I(g) of PTE 84–14 due to the Conviction, the Department would consider relevant any legal proceedings, including civil claims and lawsuits, regulatory examinations, investigations, audits, and requests for information by various governmental regulatory agencies and law enforcement authorities in various jurisdictions that may be pending at that time notwithstanding whether such proceedings would trigger ineligibility. In this regard, any such proceedings would be relevant to the Department's analysis of whether the Northern Trust QPAMs (and those who may be in a position to influence the QPAMs' policies) maintain the high standard of integrity required to operate as a QPAM.

Technical Correction

Section II(a) of PTE 2016–11 is corrected to read as follows:

"(a) The term "Conviction" means the judgment of conviction against NTFS for aiding and abetting tax fraud entered in France in the Court of Appeal, French Special Prosecutor No. 1120392066, French Investigative Judge No. JIRSIF/11/12 or another court of competent jurisdiction."

Signed at Washington, DC.

George Christopher Cosby,

Director, Office of Exemption Determinations, Employee Benefits Security Administration, U.S. Department of Labor.

[FR Doc. 2024–07128 Filed 4–3–24; 8:45 am]

BILLING CODE 4510–29–P

POSTAL REGULATORY COMMISSION

[Docket Nos. MC2024–217 and CP2024–223; MC2024–218 and CP2024–224]

New Postal Products

AGENCY: Postal Regulatory Commission.

ACTION: Notice.

SUMMARY: The Commission is noticing a recent Postal Service filing for the Commission's consideration concerning a negotiated service agreement. This notice informs the public of the filing, invites public comment, and takes other administrative steps.

DATES: *Comments are due:* April 8, 2024.

ADDRESSES: Submit comments electronically via the Commission's Filing Online system at <http://www.prc.gov>. Those who cannot submit comments electronically should contact the person identified in the **FOR FURTHER INFORMATION CONTACT** section by telephone for advice on filing alternatives.

FOR FURTHER INFORMATION CONTACT: David A. Trissell, General Counsel, at 202–789–6820.

SUPPLEMENTARY INFORMATION:

Table of Contents

- I. Introduction
- II. Docketed Proceeding(s)

I. Introduction

The Commission gives notice that the Postal Service filed request(s) for the Commission to consider matters related to negotiated service agreement(s). The request(s) may propose the addition or removal of a negotiated service agreement from the Market Dominant or the Competitive product list, or the modification of an existing product currently appearing on the Market Dominant or the Competitive product list.

Section II identifies the docket number(s) associated with each Postal Service request, the title of each Postal Service request, the request's acceptance date, and the authority cited by the Postal Service for each request. For each request, the Commission appoints an officer of the Commission to represent the interests of the general public in the proceeding, pursuant to 39 U.S.C. 505 (Public Representative). Section II also establishes comment deadline(s) pertaining to each request.

The public portions of the Postal Service's request(s) can be accessed via the Commission's website (<http://www.prc.gov>). Non-public portions of the Postal Service's request(s), if any, can be accessed through compliance with the requirements of 39 CFR 3011.301.¹

¹ See Docket No. RM2018–3, Order Adopting Final Rules Relating to Non-Public Information, June 27, 2018, Attachment A at 19–22 (Order No. 4679).

The Commission invites comments on whether the Postal Service's request(s) in the captioned docket(s) are consistent with the policies of title 39. For request(s) that the Postal Service states concern Market Dominant product(s), applicable statutory and regulatory requirements include 39 U.S.C. 3622, 39 U.S.C. 3642, 39 CFR part 3030, and 39 CFR part 3040, subpart B. For request(s) that the Postal Service states concern Competitive product(s), applicable statutory and regulatory requirements include 39 U.S.C. 3632, 39 U.S.C. 3633, 39 U.S.C. 3642, 39 CFR part 3035, and 39 CFR part 3040, subpart B. Comment deadline(s) for each request appear in section II.

II. Docketed Proceeding(s)

1. *Docket No(s)*: MC2024–217 and CP2024–223; *Filing Title*: USPS Request to Add Priority Mail & Parcel Select Contract 10 to Competitive Product List and Notice of Filing Materials Under Seal; *Filing Acceptance Date*: March 29, 2024; *Filing Authority*: 39 U.S.C. 3642, 39 CFR 3040.130 through 3040.135, and 39 CFR 3035.105; *Public Representative*: Christopher C. Mohr; *Comments Due*: April 8, 2024.

2. *Docket No(s)*: MC2024–218 and CP2024–224; *Filing Title*: USPS Request to Add Priority Mail Express, Priority Mail & USPS Ground Advantage Contract 52 to Competitive Product List and Notice of Filing Materials Under Seal; *Filing Acceptance Date*: March 29, 2024; *Filing Authority*: 39 U.S.C. 3642, 39 CFR 3040.130 through 3040.135, and 39 CFR 3035.105; *Public Representative*: Christopher C. Mohr; *Comments Due*: April 8, 2024.

This Notice will be published in the **Federal Register**.

Erica A. Barker,
Secretary.

[FR Doc. 2024–07135 Filed 4–3–24; 8:45 am]
BILLING CODE 7710–FW–P

POSTAL SERVICE

Product Change—Priority Mail and Parcel Select Negotiated Service Agreement

AGENCY: Postal Service™.
ACTION: Notice.

SUMMARY: The Postal Service gives notice of filing a request with the Postal Regulatory Commission to add a domestic shipping services contract to the list of Negotiated Service Agreements in the Mail Classification Schedule's Competitive Products List.
DATES: *Date of required notice*: April 4, 2024.

FOR FURTHER INFORMATION CONTACT: Sean C. Robinson, 202–268–8405.

SUPPLEMENTARY INFORMATION: The United States Postal Service® hereby gives notice that, pursuant to 39 U.S.C. 3642 and 3632(b)(3), on March 28, 2024, it filed with the Postal Regulatory Commission a *Request of the United States Postal Service to Add Priority Mail & Parcel Select Contract 10 to Competitive Product List*. Documents are available at www.prc.gov, Docket Nos. MC2024–217, CP2024–223.

Sean Robinson,

Attorney, Corporate and Postal Business Law.
[FR Doc. 2024–07102 Filed 4–3–24; 8:45 am]

BILLING CODE 7710–12–P

POSTAL SERVICE

Product Change—Priority Mail Express, Priority Mail, and USPS Ground Advantage® Negotiated Service Agreement

AGENCY: Postal Service™.
ACTION: Notice.

SUMMARY: The Postal Service gives notice of filing a request with the Postal Regulatory Commission to add a domestic shipping services contract to the list of Negotiated Service Agreements in the Mail Classification Schedule's Competitive Products List.
DATES: *Date of required notice*: April 4, 2024.

FOR FURTHER INFORMATION CONTACT: Sean C. Robinson, 202–268–8405.

SUPPLEMENTARY INFORMATION: The United States Postal Service® hereby gives notice that, pursuant to 39 U.S.C. 3642 and 3632(b)(3), on March 28, 2024, it filed with the Postal Regulatory Commission a *USPS Request to Add Priority Mail Express, Priority Mail & USPS Ground Advantage® Contract 52 to Competitive Product List*. Documents are available at www.prc.gov, Docket Nos. MC2024–218, CP2024–224.

Sean C. Robinson,

Attorney, Corporate and Postal Business Law.
[FR Doc. 2024–07103 Filed 4–3–24; 8:45 am]

BILLING CODE 7710–12–P

POSTAL SERVICE

Product Change—Priority Mail and USPS Ground Advantage® Negotiated Service Agreement

AGENCY: Postal Service™.
ACTION: Notice.

SUMMARY: The Postal Service gives notice of filing a request with the Postal

Regulatory Commission to add a domestic shipping services contract to the list of Negotiated Service Agreements in the Mail Classification Schedule's Competitive Products List.
DATES: *Date of required notice*: April 4, 2024.

FOR FURTHER INFORMATION CONTACT: Sean Robinson, 202–268–8405.

SUPPLEMENTARY INFORMATION: The United States Postal Service® hereby gives notice that, pursuant to 39 U.S.C. 3642 and 3632(b)(3), on March 26, 2024, it filed with the Postal Regulatory Commission a *USPS Request to Add Priority Mail & USPS Ground Advantage® Contract 207 to Competitive Product List*. Documents are available at www.prc.gov, Docket Nos. MC2024–215, CP2024–221.

Sean Robinson,

Attorney, Corporate and Postal Business Law.
[FR Doc. 2024–07100 Filed 4–3–24; 8:45 am]

BILLING CODE 7710–12–P

POSTAL SERVICE

Product Change—Priority Mail Express Negotiated Service Agreement

AGENCY: Postal Service™.
ACTION: Notice.

SUMMARY: The Postal Service gives notice of filing a request with the Postal Regulatory Commission to add a domestic shipping services contract to the list of Negotiated Service Agreements in the Mail Classification Schedule's Competitive Products List.
DATES: *Date of required notice*: April 4, 2024.

FOR FURTHER INFORMATION CONTACT: Sean Robinson, 202–268–8405.

SUPPLEMENTARY INFORMATION: The United States Postal Service® hereby gives notice that, pursuant to 39 U.S.C. 3642 and 3632(b)(3), on March 25, 2024, it filed with the Postal Regulatory Commission a *USPS Request to Add Priority Mail Express Contract 100 to Competitive Product List*. Documents are available at www.prc.gov, Docket Nos. MC2024–213, CP2024–219.

Sean Robinson,

Attorney, Corporate and Postal Business Law.
[FR Doc. 2024–07098 Filed 4–3–24; 8:45 am]

BILLING CODE 7710–12–P

POSTAL SERVICE

Product Change—Priority Mail and USPS Ground Advantage® Negotiated Service Agreement

AGENCY: Postal Service™.

ACTION: Notice.

SUMMARY: The Postal Service gives notice of filing a request with the Postal Regulatory Commission to add a domestic shipping services contract to the list of Negotiated Service Agreements in the Mail Classification Schedule's Competitive Products List.

DATES: *Date of required notice:* April 4, 2024.

FOR FURTHER INFORMATION CONTACT: Sean Robinson, 202-268-8405.

SUPPLEMENTARY INFORMATION: The United States Postal Service® hereby gives notice that, pursuant to 39 U.S.C. 3642 and 3632(b)(3), on March 26, 2024, it filed with the Postal Regulatory Commission a *USPS Request to Add Priority Mail & USPS Ground Advantage® Contract 208 to Competitive Product List*. Documents are available at www.prc.gov, Docket Nos. MC2024-216, CP2024-222.

Sean Robinson,

Attorney, Corporate and Postal Business Law.

[FR Doc. 2024-07101 Filed 4-3-24; 8:45 am]

BILLING CODE 7710-12-P

POSTAL SERVICE**Product Change—Priority Mail and USPS Ground Advantage® Negotiated Service Agreement**

AGENCY: Postal Service™.

ACTION: Notice.

SUMMARY: The Postal Service gives notice of filing a request with the Postal Regulatory Commission to add a domestic shipping services contract to the list of Negotiated Service Agreements in the Mail Classification Schedule's Competitive Products List.

DATES: *Date of required notice:* April 4, 2024.

FOR FURTHER INFORMATION CONTACT: Sean Robinson, 202-268-8405.

SUPPLEMENTARY INFORMATION: The United States Postal Service® hereby gives notice that, pursuant to 39 U.S.C. 3642 and 3632(b)(3), on March 26, 2024, it filed with the Postal Regulatory Commission a *USPS Request to Add Priority Mail & USPS Ground Advantage® Contract 206 to Competitive Product List*. Documents are available at www.prc.gov, Docket Nos. MC2024-214, CP2024-220.

Sean Robinson,

Attorney, Corporate and Postal Business Law.

[FR Doc. 2024-07099 Filed 4-3-24; 8:45 am]

BILLING CODE 7710-12-P

SMALL BUSINESS ADMINISTRATION

[Disaster Declaration #20258; MARYLAND Disaster Number MD-20001 Declaration of Economic Injury]

Administrative Declaration of an Economic Injury Disaster for the State of Maryland

AGENCY: U.S. Small Business Administration.

ACTION: Notice.

SUMMARY: This is a notice of an Economic Injury Disaster Loan (EIDL) declaration for the State of Maryland dated 03/29/2024. This catastrophe has far-ranging effects for businesses throughout the state, surrounding areas and are of national scale and significance.

Incident: Francis Scott Key Bridge Collapse.

Incident Period: 03/26/2024 and continuing.

DATES: Issued on 03/29/2024.

Economic Injury (EIDL) Loan Application Deadline Date: 12/30/2024.

ADDRESSES: Visit the MySBA Loan Portal at <https://lending.sba.gov> to apply for a disaster assistance loan.

FOR FURTHER INFORMATION CONTACT:

Vanessa Morgan, Office of Disaster Recovery & Resilience, U.S. Small Business Administration, 409 3rd Street SW, Suite 6050, Washington, DC 20416, (202) 205-6734.

SUPPLEMENTARY INFORMATION: Notice is hereby given that as a result of the Administrator's EIDL declaration, applications for disaster loans may be submitted online using the MySBA Loan Portal <https://lending.sba.gov> or other locally announced locations. Please contact the SBA disaster assistance customer service center by email a *disastercustomerservice@sba.gov* or by phone at 1-800-659-2955 for further assistance.

The following areas have been determined to be adversely affected by the disaster:

Primary Counties: Allegany, Anne Arundel, Baltimore, Baltimore, Calvert, Caroline, Carroll, Cecil, Charles, Dorchester, Frederick, Garrett, Harford, Howard, Kent, Montgomery, Prince George's, Queen Anne's, Somerset, St. Mary's, Talbot, Washington, Wicomico, Worcester.

Contiguous Counties:

Delaware: Kent, New Castle, Sussex.
District Of Columbia: District of Columbia.

Pennsylvania: Fulton, Franklin, Adams, York, Bedford, Fayette, Lancaster, Somerset, Chester.

Virginia: Arlington, Alexandria, Loudoun, Accomack, Fairfax County.

West Virginia: Morgan, Berkeley, Jefferson, Hampshire, Mineral, Grant, Preston.

The Interest Rates are:

	Percent
Business and Small Agricultural Cooperatives without Credit Available Elsewhere	4.000
Non-Profit Organizations without Credit Available Elsewhere	3.250

The number assigned to this disaster for economic injury is 202580.

The States which received an EIDL Declaration are Delaware, District of Columbia, Maryland, Pennsylvania, Virginia, West Virginia.

(Catalog of Federal Domestic Assistance Number 59008)

Isabella Guzman,

Administrator.

[FR Doc. 2024-07122 Filed 4-3-24; 8:45 am]

BILLING CODE 8026-09-P

SMALL BUSINESS ADMINISTRATION

[Disaster Declaration #20235 and #20236; INDIANA Disaster Number IN-20000]

Administrative Declaration of a Disaster for the State of Indiana

AGENCY: U.S. Small Business Administration.

ACTION: Notice.

SUMMARY: This is a notice of an Administrative declaration of a disaster for the State of Indiana dated 03/29/2024.

Incident: Severe Storms and Tornadoes.

Incident Period: 03/14/2024.

DATES: Issued on 03/29/2024.

Physical Loan Application Deadline Date: 05/28/2024.

Economic Injury (EIDL) Loan Application Deadline Date: 12/30/2024.

ADDRESSES: Visit the MySBA Loan Portal at <https://lending.sba.gov> to apply for a disaster assistance loan.

FOR FURTHER INFORMATION CONTACT: Vanessa Morgan, Office of Disaster Recovery & Resilience, U.S. Small Business Administration, 409 3rd Street SW, Suite 6050, Washington, DC 20416, (202) 205-6734.

SUPPLEMENTARY INFORMATION: Notice is hereby given that as a result of the Administrator's disaster declaration, applications for disaster loans may be submitted online using the MySBA Loan Portal <https://lending.sba.gov> or

other locally announced locations. Please contact the SBA disaster assistance customer service center by email at disastercustomerservice@sba.gov or by phone at 1-800-659-2955 for further assistance.

The following areas have been determined to be adversely affected by the disaster:

Primary Counties: Randolph.

Contiguous Counties:

Indiana: Delaware, Henry, Jay, Wayne.

Ohio: Darke.

The Interest Rates are:

	Percent
<i>For Physical Damage:</i>	
Homeowners with Credit Available Elsewhere	5.375
Homeowners without Credit Available Elsewhere	2.688
Businesses with Credit Available Elsewhere	8.000
Businesses without Credit Available Elsewhere	4.000
Non-Profit Organizations with Credit Available Elsewhere ...	3.250
Non-Profit Organizations without Credit Available Elsewhere	3.250
<i>For Economic Injury:</i>	
Business and Small Agricultural Cooperatives without Credit Available Elsewhere	4.000
Non-Profit Organizations without Credit Available Elsewhere	3.250

The number assigned to this disaster for physical damage is 20235C and for economic injury is 202360.

The States which received an EIDL Declaration are Indiana, Ohio.

(Catalog of Federal Domestic Assistance Number 59008)

Isabella Guzman,
Administrator.

[FR Doc. 2024-07124 Filed 4-3-24; 8:45 am]

BILLING CODE 8026-09-P

DEPARTMENT OF TRANSPORTATION

Federal Motor Carrier Safety Administration

[Docket No. FMCSA-2024-0097]

Agency Information Collection Activities; Emergency Approval of Revision to an Approved Information Collection Request: Apprenticeship Pilot Program

AGENCY: Federal Motor Carrier Safety Administration (FMCSA), Department of Transportation (DOT).

ACTION: Notice of request for emergency OMB approval.

SUMMARY: In compliance with the Paperwork Reduction Act (PRA) of 1995, this notice announces that the Information Collection Request (ICR) discussed below has been forwarded to the Office of Management and Budget (OMB) for review of a required revision and emergency approval. FMCSA requests approval to revise, on an emergency basis, an ICR titled, “Safe Driver Apprenticeship Pilot Program” to conform the collection with recently revised statutory authority. FMCSA requests that OMB approve this collection by April 15, 2024.

FOR FURTHER INFORMATION CONTACT: Nicole Michel, Mathematical Statistician, Research Division, DOT, FMCSA, West Building, 6th Floor, 1200 New Jersey Avenue SE, Washington, DC 20590-0001; 202-366-4354; *email:* Nicole.michel@dot.gov.

SUPPLEMENTARY INFORMATION:
Title: Safe Driver Apprenticeship Pilot Program.

OMB Control Number: 2126-0075.
Type of Request: Request for emergency approval of revisions to an existing information collection.

Respondents: Motor carriers; drivers.
Estimated Total Respondents: 14,830 total (1,600 motor carriers and 13,230 CMV drivers); 5,410 annually (1,000 carriers and 4,410 CMV drivers).

Estimated Total Responses: 168,430 total, or 56,143 annually (applications: 14,830 total, or 4,943 annually; plus data collection for participating carriers: 153,600 total, or 51,200 annually).

Estimated Burden Hours: 169,343 hours total, or 56,448 hours annually (Motor carriers: 164,933 hours total, or 54,978 hours annually; Drivers: 4,410 hours total, or 1,470 hours annually).

Estimated Burden per Response: 20 minutes per response for carrier, apprentice, and experienced driver application forms; 15 minutes per response for safety benchmark certifications; 60 minutes per month per driver for monthly driving and safety data; 90 minutes per month for miscellaneous data submission.

Frequency: Once for carrier, apprentice, and experienced driver application forms; twice per apprentice for safety benchmark certifications; monthly per number of participating drivers for driving and safety data; and monthly for miscellaneous monthly data.

Background

Current regulations on driver qualifications (49 CFR part 391.11(b)(1)) state that a driver must be 21 years of age or older to operate a CMV in interstate commerce. Currently, drivers

under the age of 21 may operate CMVs only in intrastate commerce subject to State laws and regulations.

Section 23022 of the Infrastructure Investment and Jobs Act (IIJA), requires the Secretary of Transportation to conduct a commercial driver Apprenticeship Pilot Program. An *apprentice* is defined as a person under the age of 21 who holds a commercial driver’s license (CDL). Under this program, these apprentices will complete two probationary periods, during which they may operate in interstate commerce only under the supervision of an experienced driver in the passenger seat. An *experienced* driver is defined in section 23022 as a driver who is not younger than 26 years old, who has held a CDL and been employed for at least the past 2 years, and who has at least 5 years of interstate CMV experience and meets the other safety criteria defined in the IIJA.

The first probationary period must include at least 120-hours of on duty time, of which at least 80 hours are driving time in a CMV. To complete this probationary period, the employer must determine competency in:

1. Interstate, city traffic, rural 2-lane, and evening driving;
2. Safety awareness;
3. Speed and space management;
4. Lane control;
5. Mirror Scanning;
6. Right and left turns; and
7. Logging and complying with rules relating to hours of service.

The second probationary period must include at least 280 hours of on-duty time, including not less than 160 hours driving time in a CMV. To complete this probationary period, the employer must determine competency in:

1. Backing and maneuvering in close quarters;
2. Pre-trip inspections;
3. Fueling procedures;
4. Weighing loads, weight distribution, and sliding tandems;
5. Coupling and uncoupling procedures; and
6. Trip planning, truck routes, map reading, navigation, and permits.

After completion of the second probationary period, the apprentice may begin operating CMVs in interstate commerce unaccompanied by an experienced driver.

In addition to data regarding successful completion of the probationary periods, the IIJA requires data collection and submission relating to any incident in which a participating apprentice is involved, as well as other data relating to the safety performance of apprentices. Additional data will include crash data (incident reports,

police reports, insurance reports), inspection data, citation data, safety event data (as recorded by all safety systems installed on vehicles, to include advanced driver assistance systems, automatic emergency braking systems, onboard monitoring systems, required forward-facing video systems and optional in-cab video systems, if a carrier chooses to provide this data) as well as exposure data (record of duty status logs, on-duty time, driving time, and time spent away from home terminal). This data will be submitted monthly through participating motor carriers.

The data collected will be used to report on the following items, as required by section 23022:

1. The findings and conclusions on the ability of technologies or training provided to apprentices as part of the pilot program to successfully improve safety;
2. An analysis of the safety record of participating apprentices as compared to other CMV drivers;
3. The number of drivers that discontinued participation in the apprenticeship program before completion;
4. A comparison of the safety records of participating drivers before, during, and after each probationary period; and
5. A comparison of each participating driver's average on-duty time, driving time, and time spent away from home terminal before, during, and after each probationary period.

FMCSA will monitor the monthly data being reported by the motor carriers and will identify drivers or carriers that may pose a risk to public safety. While removing unsafe drivers or carriers may bias the dataset, it is a necessary feature for FMCSA to comply with 49 CFR 381.505, which requires development of a monitoring plan to ensure adequate safeguards to protect the health and safety of pilot program participants and the general public. Knowing that a driver or carrier was removed from the pilot program for safety reasons will help FMCSA minimize bias in the final data analysis.

The statutory mandate for this pilot program is contained in section 23022 of the IJJA. FMCSA's regulatory authority for initiation of a pilot program is 49 CFR 381.400. The Apprentice Pilot Program supports the DOT strategic goal of economic strength while maintaining DOT's and FMCSA's commitment to safety.

Revision

The Consolidated Appropriations Act of 2024 (Pub. L. 118-42) revised FMCSA's authority regarding the Safe

Driver Apprenticeship Pilot (SDAP) Program. Section 422 of that Act states that FMCSA may not require the use of inward facing cameras or require a motor carrier to register an apprenticeship program with the Department of Labor as a condition for participation in the SDAP program. As such, the application and monthly report forms have been revised to remove those two elements as mandatory requirements. However, the Agency will continue to ask carriers whether they use inward facing cameras and whether they have a Registered Apprenticeship program approval number, and will give carriers the option of providing that information. Therefore, FMCSA does not expect to see any change in the number of respondents, responses, or the overall burden of this information collection.

In accordance with the PRA and OMB's implementing regulations at 5 CFR 1320.13, this information is necessary to the mission of the Agency and is needed prior to the ordinary time periods established for revision of an approved collection of information (found within 5 CFR part 1320). The Agency cannot reasonably comply with the normal clearance procedures listed under this part because the use of normal clearance procedures is reasonably likely to cause a statutory deadline to be missed (5 CFR 1320.13(2)(iii)).

Issued under the authority delegated in 49 CFR 1.87.

Thomas P. Keane,

Associate Administrator, Office of Research and Registration.

[FR Doc. 2024-07172 Filed 4-3-24; 8:45 am]

BILLING CODE 4910-EX-P

DEPARTMENT OF TRANSPORTATION

Federal Transit Administration

[Docket No. FTA-2024-0004]

Rural Areas Formula Grant Programs Guidance Proposed Circular

AGENCY: Federal Transit Administration (FTA), Department of Transportation (DOT).

ACTION: Notice of availability of proposed circular updates and request for comments.

SUMMARY: The Federal Transit Administration (FTA) has placed in the docket and on its website, proposed guidance in the form of an updated circular, to assist recipients in their implementation of the Rural Areas Formula Program and the rural component of the Buses and Bus

Facilities Program. The purpose of these proposed updates is to provide recipients of FTA financial assistance with updated guidance on program administration. The proposed revisions to these circulars are a result of changes in the law since the last updates to both the Rural Areas and Buses and Bus Facilities circulars. By this notice, FTA invites public comment on the proposed circular.

DATES: Comments must be submitted by June 3, 2024. Late-filed comments will be considered to the extent practicable.

ADDRESSES: Please submit your comments by only one of the following methods, identifying your submission by docket number FTA-2024-0004. All electronic submissions must be made to the U.S. Government electronic site at <https://www.regulations.gov/>.

(1) *Federal eRulemaking Portal:* Go to <https://www.regulations.gov/> and follow the online instructions for submitting comments.

(2) *Mail:* Docket Management Facility: U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building, Ground Floor, Room W12-140, Washington, DC 20590-0001.

(3) *Hand Delivery or Courier:* West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE, between 9 a.m. and 5 p.m. Eastern time, Monday through Friday, except Federal holidays.

(4) *Fax:* 202-493-2251.

Instructions: You must include the agency name (Federal Transit Administration) and Docket number (FTA-2024-0004) for this notice at the beginning of your comments. Submit two copies of your comments if you submit them by mail. For confirmation that FTA received your comments, include a self-addressed stamped postcard. Note that all comments received will be posted without change to <https://www.regulations.gov/> including any personal information provided and will be available to internet users. For information on DOT's compliance with the Privacy Act, please visit <https://www.transportation.gov/privacy>.

Docket: For access to the docket to read background documents and comments received, go to <https://www.regulations.gov/> at any time or to the U.S. Department of Transportation, 1200 New Jersey Ave. SE, Docket Operations, M-30, West Building Ground Floor, Room W12-140, Washington, DC 20590 between 9 a.m. and 5 p.m. Eastern Time, Monday through Friday, except Federal holidays.

FOR FURTHER INFORMATION CONTACT: For program questions, Jay Lindsey, Office of Program Management, phone, (202)

366–6299 or email, Jay.Lindsey@dot.gov. For legal questions, Bonnie Graves, Office of Chief Counsel, phone, (202) 366–0944, or email, Bonnie.Graves@dot.gov.

SUPPLEMENTARY INFORMATION:

Table of Contents

- I. Overview
- II. Chapter-by-Chapter Analysis
 - A. Chapter I—Introduction and Background
 - B. Chapter II—Program Overview
 - C. Chapter III—General Program Information
 - D. Chapter IV—Eligible Projects and Requirements
 - E. Chapter V—Planning and Program Development
 - F. Chapter VI—Program Management and Administrative Requirements
 - G. Chapter VII—State Management Plan
 - H. Chapter VIII—Appalachian Development Public Transportation Assistance Program (ADTAP)
 - I. Chapter IX—Intercity Bus
 - J. Chapter X—Rural Transportation Assistance Program (RTAP)
 - K. Chapter XI—Public Transportation on Indian Reservations
 - L. Appendices

I. Overview

The Federal Transit Administration’s (FTA) proposed circular, “Rural Areas Formula Grant Programs Guidance,” C 9040.1H, is a consolidation of guidance for the administration and preparation of grant applications for the Rural Areas Formula Grants Program under 49 U.S.C. 5311 (FTA circular 9040.1) and the rural area component of the Grants for Buses and Bus Facilities Program under 49 U.S.C. 5339(a) (FTA circular 5100.1). Additionally, this updated circular incorporates provisions of the FAST Act (Pub. L. 114–94), the Infrastructure Investment and Jobs Act (IIJA) (Pub. L. 117–58), and other changes in law, and includes program-specific guidance for these formula programs. Additional requirements for all grant programs are identified in FTA’s Award Management Requirements circular 5010.1. The availability of the proposed 5010 circular and request for public comment was published in the **Federal Register** (89 FR 11334, Feb. 14, 2024) and is posted on <https://www.regulations.gov> in Docket FTA–2024–0003.

The proposed update to circular 9040.1 consolidates and summarizes programmatic information, streamlines pre-existing guidance from the two program circulars, and reduces duplication of information provided between the Rural Areas Formula Program circular and FTA’s other topic-specific circulars, including by moving certain text applicable to most or all of

FTA’s grant programs to FTA’s Award Management Requirements circular 5010.1. Furthermore, the proposed circular incorporates statutory changes and clarifies a number of policy issues as interpreted and applied by FTA. Statutory changes for section 5311 include additional sources of local share; in-kind match for intercity bus service; and fund allocations for tribes. Statutory changes for section 5339(a) include the application of section 5311 requirements to section 5339 grants in rural areas; additional source for local share; additional eligible entities; and use of procurement tools authorized under section 3019 of the FAST Act. Policy clarifications address topics in the existing program circulars, including consolidation of grants to insular areas; eligible projects and activities for each formula program; operating assistance limitations and exceptions; capital cost of contracting; the role of transportation network companies in providing public transportation services; and period of availability to obligate funds flexed to FTA formula programs from the Federal Highway Administration (FHWA).

In addition to statutory and policy updates, the Office of Management and Budget (OMB) issued 2 CFR part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, also known as the Uniform Guidance, in December 2013, which superseded the Common Grant Rule, formerly codified at 49 CFR parts 18 and 19. Due to the timing of the last circular update and the effective date of the Uniform Guidance, FTA circular 9040.1G continued to reference 49 CFR parts 18 and 19. FTA has updated these references, including definitions, in proposed circular 9040.1H.

This notice provides a summary of proposed changes to the current circular 9040.1G, “Formula Grants for Rural Areas: Program Guidance and Grant Application Instructions.” FTA invites public comment on the substance and format of the proposed circular.

A. Chapter I—Introduction and Background

Due to the consolidation of the two program circulars, definitions and program descriptions were compared and revised for consistency with proposed updates to circular 5010.1E “Award Management Requirements,” circular 9030.1E “Formula Grants for Urbanized Areas,” and circular 9070.1G “Enhanced Mobility of Seniors and Individuals with Disabilities.” FTA proposes to amend the definitions section for consistency, clarification,

and to reflect changes in statutes and other authorities. For example, FTA has updated the following terms: “Capital Asset” is modified for consistency with Generally Accepted Accounting Principles (GAAP), Governmental Accounting Standards Board (GASB), Financial Accounting Standards Board (FASB), and FTA’s Uniform System of Accounts. “Clean Fuel Bus” recognizes low or no emissions technologies other than full electric and hybrid electric buses. “Rehabilitate” is expanded to include applicability to bus facilities and amended to clarify that not all rehabilitative activities must be a restoration to original condition, to more accurately reflect the term’s broad usage in 49 U.S.C. 5339. “Urbanized Area” is updated to reflect changes in designation by the U.S. Census Bureau, which no longer utilizes “Urbanized Area” (UZA) but instead uses “Urban Area,” as defined by the Secretary of Commerce. “Useful Life” now applies to real property and other capital assets. Because useful life depends on depreciation and estimated time in use, consideration of useful life varies according to the type of asset in question.

B. Chapter II—Program Overview

Chapter II of the proposed circular contains information related to program goals, State and FTA roles in program administration, and relationship of the section 5311 program to other programs. These sections are in the current 9040.1G circular and the language is generally unchanged, with updates where appropriate. Consistent with the consolidation of section 5339 program requirements into the new circular, the updated chapter contains information related to section 5339 as well as section 5311. FTA proposes to add a section on program measures with broad measures for both section 5311 and section 5339. In addition, FTA proposes a new section on program oversight.

C. Chapter III—General Program Information

FTA proposes substantially reorganizing the material found in Chapters III–V of circular 9040.1G, consistent with the reorganization of the Urbanized Area Program circular. Material in Chapters III–V of circular 9040.1G not moved to circular 5010.1 generally is in Chapters III–VI of the proposed circular. For example, some of the information contained in Chapter III of the current circular remains in this chapter, and other information moves to Chapter IV. Eligible recipients, apportionment of funds, and local share of project costs remain in Chapter III,

but in a different order. FTA has clarified in the updated circular that local share is waived for insular areas. FTA proposes moving eligible activities, including discussions related to job access/reverse commute, operating, administrative, and capital expenses, to Chapter IV. A new section in Chapter III discusses the eligibility of rural funds for use in urbanized areas. In addition, we have included a section on taxis and transportation network companies, and when these entities may be subrecipients or contractors. This section has been in FTA's 9070.1 circular for many years and is slightly modified for the section 5311 program. FTA has historically treated transportation network companies (TNCs) the same as taxis, given they both provide on-demand, exclusive ride service, primarily in automobiles. Where taxis and TNCs provide shared ride service, they may be subrecipients. Exclusive-ride companies may be contractors for job access reverse commute (JARC) service under section 5311, as eligible JARC activities include service that does not meet the definition of "public transportation" in 49 U.S.C. 5302(15).

D. Chapter IV—Eligible Projects and Requirements

Chapter IV in circular 9040.1G is titled "Program Development." As stated above, FTA proposes moving some of the information found in Chapter III of the existing circular to Chapter IV. In addition, we propose moving much of the information found in Chapter IV of circular 9040.1G to Chapter V of circular 9040.1H. Chapter IV in the updated circular includes information related to eligible projects. Given the consolidation of the Rural Areas and Buses and Bus Facilities circulars, this chapter specifies which activities are eligible under each of the programs. Capital leases to replace vehicles are eligible, and in the event a contractor is used to provide service, the actual costs of a capital lease can be removed from the operating contract and funded at an 80 percent federal share, or the recipient can utilize capital cost of contracting. FTA proposes two new sections: employee training expenses, and interest and debt financing as an eligible cost. FTA proposes moving information related to certifications and assurances, pre-award authority and grant award and project approval to FTA circular 5010.1.

E. Chapter V—Planning and Program Development

The proposed circular moves much of the information found in Chapter V of

circular 9040.1G, to FTA's circular 5010.1, Award Management Requirements, including information on procurement, financial management, data universal numbering system (DUNS), system for awards management (SAM), electronic clearinghouse operation (ECHO), and other topics that apply to all FTA grant programs. Most of the information not moved to circular 5010.1 is moved to Chapter VI of the proposed circular 9040.1H, including satisfactory continuing control, state financial records, reporting requirements and the state management plan.

FTA proposes moving much of the information in Chapter IV of circular 9040.1G, including fair and equitable distribution of funds, planning requirements, performance-based planning, intercity bus consultation, program of projects, to proposed Chapter V of circular 9040.1H. Chapter V includes a reference to pre-award authority, but the full discussion is included in FTA Circular 5010.1. The proposed Chapter V also includes information related to coordinated planning, availability of FHWA funds flexed to transit projects, transit asset management requirements, public transit safety requirements, and environmental considerations. As with other chapters, FTA has updated this chapter to include references to section 5339 as appropriate. The chapter contains updates and clarifications to the program of projects and coordinated planning requirements. FTA proposes updating the section describing flex funding from FHWA and includes a period of availability for funds that are transferred. FTA proposes moving sections on transit asset management and safety from Chapter XI of circular 9040.1G to this chapter and has updated the text consistent with changes in law and with the transit asset management and safety regulations issued after the last circular update.

F. Chapter VI—Program Management and Administrative Requirements

Chapter VI of circular 9040.1G is the state management plan; FTA proposes moving this to Chapter VII. The new Chapter VI contains information on satisfactory continuing control and responsibility, state financial records, construction management and oversight, reporting requirements, state management plan, and FTA state management plan review. FTA proposes adding references to section 5339 as appropriate; the substance of these sections is substantially similar to these sections in the current circulars.

G. Chapter VII—State Management Plan

Proposed Chapter VII is substantially similar to Chapter VI of circular 9040.1G, except it adds references to section 5339 and removes the section on State Management Plan Reviews, which is moved to Chapter VI. Thus, Chapter VII includes general information, a statement regarding the purpose of state management plans, the contents of state management plans, and making state management plan revisions.

H. Chapter VIII—Appalachian Development Public Transportation Assistance Program (ADTAP)

Proposed Chapter VIII is substantially similar to Chapter VII of circular 9040.1G. FTA proposes removing text related to eligible projects, local share, and planning requirements, and instead includes the statement that all requirements and eligibilities for section 5311 apply to ADTAP funds.

I. Chapter IX—Intercity Bus

Proposed Chapter IX is substantially similar to Chapter VIII in the current FTA circular 9040.1G, with the exceptions stated here. FTA has updated the section on in-kind match to reflect a change in the law. Intercity bus projects that include both feeder service and an unsubsidized segment of intercity bus service to which the feeder service connects, may use all operating and capital costs of unsubsidized segments, whether or not offset by revenue from such service, as an in-kind match for the operating costs of connecting rural intercity bus feeder service funded under section 5311(f). This section provides an example of how to calculate this in-kind match. In the section describing eligible services and service areas, FTA clarifies long-standing policy that a service is considered "commuter service" (and therefore does not meet the 15 percent intercity bus requirement of section 5311(f)) if at least 50 percent of passengers make a return trip on the same day across all service runs for one year. Finally, FTA has added text stating that private operators providing intercity service using vehicles other than over-the-road-buses are subject to the U.S. DOT Americans with Disabilities Act (ADA) regulations governing fixed route or demand responsive service by private entities.

J. Chapter X—Rural Transportation Assistance Program (RTAP)

Proposed Chapter X is substantially similar to Chapter IX in circular 9040.1G, except the section on the national program is enhanced to include more specific elements.

K. Chapter XI—Public Transportation on Indian Reservations

FTA proposes moving most of the content of Chapter XI (“Other Provisions”) in circular 9040.1G to circular 5010.1, as the cross-cutting requirements summarized in that chapter apply to most or all of FTA’s grant programs. Proposed Chapter XI is substantially similar to Chapter X in circular 9040.1G, with the exceptions stated here. There is a new paragraph on tribal self-governance, and how funds provided to a tribe with a self-governance compact between the tribe and U.S. DOT will be administered. In the section on eligible services and service areas, FTA clarifies that funds provided to tribes must be used to serve the general population in rural areas, and not just tribal members. In the section on matching requirements, the requirement has changed from an automatic 10 percent local match requirement for competitive funds to a variance depending on the allocation year. Local match requirements will be stated in notices of funding opportunity. Finally, FTA has updated the section related to indirect cost rate.

L. Appendices

FTA proposes to move most of the appendices currently found in circular 9040.1G to FTA circular 5010.1. The remaining appendices include Appendix A, Procedures Related to Flexible Funding, and Appendix B, Sample Intercity Bus Certification. Appendix A is updated consistent with changes in the law and adding a period of availability to funds flexed from FHWA. Appendix B is substantially unchanged from the intercity bus certification appendix in circular 9040.1G.

FTA invites public comment on the structure and content of proposed circular 9040.1H.

After a review and consideration of the comments provided on this proposed circular, FTA will publish the updated circular on its website and will announce the availability of the updated circular and the response to comments in the **Federal Register**.

Note that on October 5, 2023, the Office of Management and Budget (OMB) published a notice of proposed rulemaking in the **Federal Register** to revise 2 CFR part 200 and other OMB guidance for grants and agreements (88 FR 69390). FTA intends to incorporate any changes in 2 CFR part 200 to the extent OMB issues the final rule before

FTA publishes the final updated circular.

Veronica Vanterpool,
Acting Administrator.

[FR Doc. 2024–07107 Filed 4–3–24; 8:45 am]

BILLING CODE 4910–57–P

DEPARTMENT OF TRANSPORTATION

Maritime Administration

[Docket No. MARAD–2024–0049]

Coastwise Endorsement Eligibility Determination for a Foreign-Built Vessel: KIRIN (Sail); Invitation for Public Comments

AGENCY: Maritime Administration, DOT.
ACTION: Notice.

SUMMARY: The Secretary of Transportation, as represented by the Maritime Administration (MARAD), is authorized to issue coastwise endorsement eligibility determinations for foreign-built vessels which will carry no more than twelve passengers for hire. A request for such a determination has been received by MARAD. By this notice, MARAD seeks comments from interested parties as to any effect this action may have on U.S. vessel builders or businesses in the U.S. that use U.S.-flag vessels. Information about the requestor’s vessel, including a brief description of the proposed service, is listed below.

DATES: Submit comments on or before May 6, 2024.

ADDRESSES: You may submit comments identified by DOT Docket Number MARAD–2024–0049 by any one of the following methods:

- *Federal eRulemaking Portal:* Go to <https://www.regulations.gov>. Search MARAD–2024–0049 and follow the instructions for submitting comments.

- *Mail or Hand Delivery:* Docket Management Facility is in the West Building, Ground Floor of the U.S. Department of Transportation. The Docket Management Facility location address is U.S. Department of Transportation, MARAD–2024–0049, 1200 New Jersey Avenue SE, West Building, Room W12–140, Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except on Federal holidays.

Note: If you mail or hand-deliver your comments, we recommend that you include your name and a mailing address, an email address, or a telephone number in the body of your document so that we can contact you if we have questions regarding your submission.

Instructions: All submissions received must include the agency name and specific docket number. All comments received will be posted without change to the docket at www.regulations.gov, including any personal information provided. For detailed instructions on submitting comments, or to submit comments that are confidential in nature, see the section entitled Public Participation.

FOR FURTHER INFORMATION CONTACT: Patricia Hagerty, U.S. Department of Transportation, Maritime Administration, 1200 New Jersey Avenue SE, Room W23–461, Washington, DC 20590. Telephone: (202) 366–0903. Email: patricia.hagerty@dot.gov.

SUPPLEMENTARY INFORMATION: As described in the application, the intended service of the vessel KIRIN is:

—*Intended Commercial Use of Vessel:*

Requester intends to offer passenger yacht rentals and charters.

—*Geographic Region Including Base of Operations:* California. Base of Operations: Marina del Ray, California.

—*Vessel Length and Type:* 50.8’ sail

The complete application is available for review identified in the DOT docket as MARAD 2024–0049 at <https://www.regulations.gov>. Interested parties may comment on the effect this action may have on U.S. vessel builders or businesses in the U.S. that use U.S.-flag vessels. If MARAD determines, in accordance with 46 U.S.C. 12121 and MARAD’s regulations at 46 CFR part 388, that the employment of the vessel in the coastwise trade to carry no more than 12 passengers will have an unduly adverse effect on a U.S.-vessel builder or a business that uses U.S.-flag vessels in that business, MARAD will not issue an approval of the vessel’s coastwise endorsement eligibility. Comments should refer to the vessel name, state the commenter’s interest in the application, and address the eligibility criteria given in section 388.4 of MARAD’s regulations at 46 CFR part 388.

Public Participation

How do I submit comments?

Please submit your comments, including the attachments, following the instructions provided under the above heading entitled **ADDRESSES**. Be advised that it may take a few hours or even days for your comment to be reflected on the docket. In addition, your comments must be written in English. We encourage you to provide concise comments and you may attach additional documents as necessary.

There is no limit on the length of the attachments.

Where do I go to read public comments, and find supporting information?

Go to the docket online at <https://www.regulations.gov>, keyword search MARAD–2024–0049 or visit the Docket Management Facility (see **ADDRESSES** for hours of operation). We recommend that you periodically check the Docket for new submissions and supporting material.

Will my comments be made available to the public?

Yes. Be aware that your entire comment, including your personal identifying information, will be made publicly available.

May I submit comments confidentially?

If you wish to submit comments under a claim of confidentiality, you should submit the information you claim to be confidential commercial information by email to SmallVessels@dot.gov. Include in the email subject heading “Contains Confidential Commercial Information” or “Contains CCI” and state in your submission, with specificity, the basis for any such confidential claim highlighting or denoting the CCI portions. If possible, please provide a summary of your submission that can be made available to the public.

In the event MARAD receives a Freedom of Information Act (FOIA) request for the information, procedures described in the Department’s FOIA regulation at 49 CFR 7.29 will be followed. Only information that is ultimately determined to be confidential under those procedures will be exempt from disclosure under FOIA.

Privacy Act

Anyone can search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). For information on DOT’s compliance with the Privacy Act, please visit <https://www.transportation.gov/privacy>.

(Authority: 49 CFR 1.93(a), 46 U.S.C. 55103, 46 U.S.C. 12121)

By Order of the Maritime Administrator.

T. Mitchell Hudson, Jr.,

Secretary, Maritime Administration.

[FR Doc. 2024–07144 Filed 4–3–24; 8:45 am]

BILLING CODE 4910–81–P

DEPARTMENT OF TRANSPORTATION

Maritime Administration

[Docket No. MARAD–2024–0050]

Coastwise Endorsement Eligibility Determination for a Foreign-Built Vessel: UNDER OFFER (Motor); Invitation for Public Comments

AGENCY: Maritime Administration, DOT.
ACTION: Notice.

SUMMARY: The Secretary of Transportation, as represented by the Maritime Administration (MARAD), is authorized to issue coastwise endorsement eligibility determinations for foreign-built vessels which will carry no more than twelve passengers for hire. A request for such a determination has been received by MARAD. By this notice, MARAD seeks comments from interested parties as to any effect this action may have on U.S. vessel builders or businesses in the U.S. that use U.S.-flag vessels. Information about the requestor’s vessel, including a brief description of the proposed service, is listed below.

DATES: Submit comments on or before May 6, 2024.

ADDRESSES: You may submit comments identified by DOT Docket Number MARAD–2024–0050 by any one of the following methods:

- *Federal eRulemaking Portal:* Go to <https://www.regulations.gov>. Search MARAD–2024–0050 and follow the instructions for submitting comments.

- *Mail or Hand Delivery:* Docket Management Facility is in the West Building, Ground Floor of the U.S. Department of Transportation. The Docket Management Facility location address is U.S. Department of Transportation, MARAD–2024–0050, 1200 New Jersey Avenue SE, West Building, Room W12–140, Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except on Federal holidays.

Note: If you mail or hand-deliver your comments, we recommend that you include your name and a mailing address, an email address, or a telephone number in the body of your document so that we can contact you if we have questions regarding your submission.

Instructions: All submissions received must include the agency name and specific docket number. All comments received will be posted without change to the docket at www.regulations.gov, including any personal information provided. For detailed instructions on submitting comments, or to submit comments that are confidential in

nature, see the section entitled Public Participation.

FOR FURTHER INFORMATION CONTACT: Patricia Hagerty, U.S. Department of Transportation, Maritime Administration, 1200 New Jersey Avenue SE, Room W23–461, Washington, DC 20590. Telephone: (202) 366–0903. Email: patricia.hagerty@dot.gov.

SUPPLEMENTARY INFORMATION: As described in the application, the intended service of the vessel UNDER OFFER is:

Intended Commercial Use of Vessel: Requester intends to offer fishing charters.

Geographic Region Including Base of Operations: Puerto Rico. Base of Operations: San Juan, Puerto Rico.

Vessel Length and Type: 33’ motor vessel.

The complete application is available for review identified in the DOT docket as MARAD 2024–0050 at <https://www.regulations.gov>. Interested parties may comment on the effect this action may have on U.S. vessel builders or businesses in the U.S. that use U.S.-flag vessels. If MARAD determines, in accordance with 46 U.S.C. 12121 and MARAD’s regulations at 46 CFR part 388, that the employment of the vessel in the coastwise trade to carry no more than 12 passengers will have an unduly adverse effect on a U.S.-vessel builder or a business that uses U.S.-flag vessels in that business, MARAD will not issue an approval of the vessel’s coastwise endorsement eligibility. Comments should refer to the vessel name, state the commenter’s interest in the application, and address the eligibility criteria given in section 388.4 of MARAD’s regulations at 46 CFR part 388.

Public Participation

How do I submit comments?

Please submit your comments, including the attachments, following the instructions provided under the above heading entitled **ADDRESSES**. Be advised that it may take a few hours or even days for your comment to be reflected on the docket. In addition, your comments must be written in English. We encourage you to provide concise comments and you may attach additional documents as necessary. There is no limit on the length of the attachments.

Where do I go to read public comments, and find supporting information?

Go to the docket online at <https://www.regulations.gov>, keyword search MARAD–2024–0050 or visit the Docket Management Facility (see **ADDRESSES** for

hours of operation). We recommend that you periodically check the Docket for new submissions and supporting material.

Will my comments be made available to the public?

Yes. Be aware that your entire comment, including your personal identifying information, will be made publicly available.

May I submit comments confidentially?

If you wish to submit comments under a claim of confidentiality, you should submit the information you claim to be confidential commercial information by email to SmallVessels@dot.gov. Include in the email subject heading "Contains Confidential Commercial Information" or "Contains CCI" and state in your submission, with specificity, the basis for any such confidential claim highlighting or denoting the CCI portions. If possible, please provide a summary of your submission that can be made available to the public.

In the event MARAD receives a Freedom of Information Act (FOIA) request for the information, procedures described in the Department's FOIA regulation at 49 CFR 7.29 will be followed. Only information that is ultimately determined to be confidential under those procedures will be exempt from disclosure under FOIA.

Privacy Act

Anyone can search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). For information on DOT's compliance with the Privacy Act, please visit <https://www.transportation.gov/privacy>.

(Authority: 49 CFR 1.93(a), 46 U.S.C. 55103, 46 U.S.C. 12121)

By Order of the Maritime Administrator.

T. Mitchell Hudson, Jr.,

Secretary, Maritime Administration.

[FR Doc. 2024-07141 Filed 4-3-24; 8:45 am]

BILLING CODE 4910-81-P

DEPARTMENT OF TRANSPORTATION

Maritime Administration

[Docket No. MARAD-2024-0047]

Coastwise Endorsement Eligibility Determination for a Foreign-Built Vessel: RMM JOB (Motor); Invitation for Public Comments

AGENCY: Maritime Administration, DOT.
ACTION: Notice.

SUMMARY: The Secretary of Transportation, as represented by the Maritime Administration (MARAD), is authorized to issue coastwise endorsement eligibility determinations for foreign-built vessels which will carry no more than twelve passengers for hire. A request for such a determination has been received by MARAD. By this notice, MARAD seeks comments from interested parties as to any effect this action may have on U.S. vessel builders or businesses in the U.S. that use U.S.-flag vessels. Information about the requestor's vessel, including a brief description of the proposed service, is listed below.

DATES: Submit comments on or before May 6, 2024.

ADDRESSES: You may submit comments identified by DOT Docket Number MARAD-2024-0047 by any one of the following methods:

- *Federal eRulemaking Portal:* Go to <https://www.regulations.gov>. Search MARAD-2024-0047 and follow the instructions for submitting comments.
- *Mail or Hand Delivery:* Docket Management Facility is in the West Building, Ground Floor of the U.S. Department of Transportation. The Docket Management Facility location address is U.S. Department of Transportation, MARAD-2024-0047, 1200 New Jersey Avenue SE, West Building, Room W12-140, Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except on Federal holidays.

Note: If you mail or hand-deliver your comments, we recommend that you include your name and a mailing address, an email address, or a telephone number in the body of your document so that we can contact you if we have questions regarding your submission.

Instructions: All submissions received must include the agency name and specific docket number. All comments received will be posted without change to the docket at www.regulations.gov, including any personal information provided. For detailed instructions on submitting comments, or to submit comments that are confidential in

nature, see the section entitled Public Participation.

FOR FURTHER INFORMATION CONTACT: Patricia Hagerty, U.S. Department of Transportation, Maritime Administration, 1200 New Jersey Avenue SE, Room W23-461, Washington, DC 20590. Telephone: (202) 366-0903. Email: patricia.hagerty@dot.gov.

SUPPLEMENTARY INFORMATION: As described in the application, the intended service of the vessel RMM JOB is:

Intended Commercial Use of Vessel: Requester intends to offer sunset cruises in the Miami area.

Geographic Region Including Base of Operations: Florida. Base of Operations: Miami Beach, Florida.

Vessel Length and Type: 73.3' pleasure yacht.

The complete application is available for review identified in the DOT docket as MARAD 2024-0047 at <https://www.regulations.gov>. Interested parties may comment on the effect this action may have on U.S. vessel builders or businesses in the U.S. that use U.S.-flag vessels. If MARAD determines, in accordance with 46 U.S.C. 12121 and MARAD's regulations at 46 CFR part 388, that the employment of the vessel in the coastwise trade to carry no more than 12 passengers will have an unduly adverse effect on a U.S.-vessel builder or a business that uses U.S.-flag vessels in that business, MARAD will not issue an approval of the vessel's coastwise endorsement eligibility. Comments should refer to the vessel name, state the commenter's interest in the application, and address the eligibility criteria given in section 388.4 of MARAD's regulations at 46 CFR part 388.

Public Participation

How do I submit comments?

Please submit your comments, including the attachments, following the instructions provided under the above heading entitled **ADDRESSES**. Be advised that it may take a few hours or even days for your comment to be reflected on the docket. In addition, your comments must be written in English. We encourage you to provide concise comments and you may attach additional documents as necessary. There is no limit on the length of the attachments.

Where do I go to read public comments, and find supporting information?

Go to the docket online at <https://www.regulations.gov>, keyword search MARAD-2024-0047 or visit the Docket Management Facility (see **ADDRESSES** for

hours of operation). We recommend that you periodically check the Docket for new submissions and supporting material.

Will my comments be made available to the public?

Yes. Be aware that your entire comment, including your personal identifying information, will be made publicly available.

May I submit comments confidentially?

If you wish to submit comments under a claim of confidentiality, you should submit the information you claim to be confidential commercial information by email to SmallVessels@dot.gov. Include in the email subject heading "Contains Confidential Commercial Information" or "Contains CCI" and state in your submission, with specificity, the basis for any such confidential claim highlighting or denoting the CCI portions. If possible, please provide a summary of your submission that can be made available to the public.

In the event MARAD receives a Freedom of Information Act (FOIA) request for the information, procedures described in the Department's FOIA regulation at 49 CFR 7.29 will be followed. Only information that is ultimately determined to be confidential under those procedures will be exempt from disclosure under FOIA.

Privacy Act

Anyone can search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). For information on DOT's compliance with the Privacy Act, please visit <https://www.transportation.gov/privacy>.

(Authority: 49 CFR 1.93(a), 46 U.S.C. 55103, 46 U.S.C. 12121)

By Order of the Maritime Administrator.

T. Mitchell Hudson, Jr.,

Secretary, Maritime Administration.

[FR Doc. 2024-07142 Filed 4-3-24; 8:45 am]

BILLING CODE 4910-81-P

DEPARTMENT OF TRANSPORTATION

Maritime Administration

[Docket No. MARAD-2024-0051]

Coastwise Endorsement Eligibility Determination for a Foreign-Built Vessel: DREAM (Motor); Invitation for Public Comments

AGENCY: Maritime Administration, DOT.

ACTION: Notice.

SUMMARY: The Secretary of Transportation, as represented by the Maritime Administration (MARAD), is authorized to issue coastwise endorsement eligibility determinations for foreign-built vessels which will carry no more than twelve passengers for hire. A request for such a determination has been received by MARAD. By this notice, MARAD seeks comments from interested parties as to any effect this action may have on U.S. vessel builders or businesses in the U.S. that use U.S.-flag vessels. Information about the requestor's vessel, including a brief description of the proposed service, is listed below.

DATES: Submit comments on or before May 6, 2024.

ADDRESSES: You may submit comments identified by DOT Docket Number MARAD-2024-0051 by any one of the following methods:

- *Federal eRulemaking Portal:* Go to <https://www.regulations.gov>. Search MARAD-2024-0051 and follow the instructions for submitting comments.
- *Mail or Hand Delivery:* Docket Management Facility is in the West Building, Ground Floor of the U.S. Department of Transportation. The Docket Management Facility location address is U.S. Department of Transportation, MARAD-2024-0051, 1200 New Jersey Avenue SE, West Building, Room W12-140, Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except on Federal holidays.

Note: If you mail or hand-deliver your comments, we recommend that you include your name and a mailing address, an email address, or a telephone number in the body of your document so that we can contact you if we have questions regarding your submission.

Instructions: All submissions received must include the agency name and specific docket number. All comments received will be posted without change to the docket at www.regulations.gov, including any personal information provided. For detailed instructions on submitting comments, or to submit comments that are confidential in nature, see the section entitled Public Participation.

FOR FURTHER INFORMATION CONTACT:

Patricia Hagerty, U.S. Department of Transportation, Maritime Administration, 1200 New Jersey Avenue SE, Room W23-461, Washington, DC 20590. Telephone: (202) 366-0903. Email: patricia.hagerty@dot.gov.

SUPPLEMENTARY INFORMATION: As described in the application, the intended service of the vessel DREAM is:

Intended Commercial Use of Vessel: Requester intends to offer hourly charters around Miami.

Geographic Region Including Base of Operations: Florida. Base of Operations: Miami, Florida.

Vessel Length and Type: 78.6' motor vessel.

The complete application is available for review identified in the DOT docket as MARAD 2024-0051 at <https://www.regulations.gov>. Interested parties may comment on the effect this action may have on U.S. vessel builders or businesses in the U.S. that use U.S.-flag vessels. If MARAD determines, in accordance with 46 U.S.C. 12121 and MARAD's regulations at 46 CFR part 388, that the employment of the vessel in the coastwise trade to carry no more than 12 passengers will have an unduly adverse effect on a U.S.-vessel builder or a business that uses U.S.-flag vessels in that business, MARAD will not issue an approval of the vessel's coastwise endorsement eligibility. Comments should refer to the vessel name, state the commenter's interest in the application, and address the eligibility criteria given in section 388.4 of MARAD's regulations at 46 CFR part 388.

Public Participation

How do I submit comments?

Please submit your comments, including the attachments, following the instructions provided under the above heading entitled **ADDRESSES**. Be advised that it may take a few hours or even days for your comment to be reflected on the docket. In addition, your comments must be written in English. We encourage you to provide concise comments and you may attach additional documents as necessary. There is no limit on the length of the attachments.

Where do I go to read public comments, and find supporting information?

Go to the docket online at <https://www.regulations.gov>, keyword search MARAD-2024-0051 or visit the Docket Management Facility (see **ADDRESSES** for hours of operation). We recommend that you periodically check the Docket for new submissions and supporting material.

Will my comments be made available to the public?

Yes. Be aware that your entire comment, including your personal identifying information, will be made publicly available.

May I submit comments confidentially?

If you wish to submit comments under a claim of confidentiality, you should submit the information you claim to be confidential commercial information by email to SmallVessels@dot.gov. Include in the email subject heading “Contains Confidential Commercial Information” or “Contains CCI” and state in your submission, with specificity, the basis for any such confidential claim highlighting or denoting the CCI portions. If possible, please provide a summary of your submission that can be made available to the public.

In the event MARAD receives a Freedom of Information Act (FOIA) request for the information, procedures described in the Department’s FOIA regulation at 49 CFR 7.29 will be followed. Only information that is ultimately determined to be confidential under those procedures will be exempt from disclosure under FOIA.

Privacy Act

Anyone can search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). For information on DOT’s compliance with the Privacy Act, please visit <https://www.transportation.gov/privacy>.

(Authority: 49 CFR 1.93(a), 46 U.S.C. 55103, 46 U.S.C. 12121)

By Order of the Maritime Administrator.

T. Mitchell Hudson, Jr.,

Secretary, Maritime Administration.

[FR Doc. 2024–07145 Filed 4–3–24; 8:45 am]

BILLING CODE 4910–81–P

DEPARTMENT OF TRANSPORTATION**Maritime Administration**

[Docket No. MARAD–2024–0048]

Coastwise Endorsement Eligibility Determination for a Foreign-Built Vessel: ICHTHYS (Motor); Invitation for Public Comments

AGENCY: Maritime Administration, DOT.

ACTION: Notice.

SUMMARY: The Secretary of Transportation, as represented by the Maritime Administration (MARAD), is authorized to issue coastwise endorsement eligibility determinations for foreign-built vessels which will carry no more than twelve passengers for hire. A request for such a determination has been received by MARAD. By this

notice, MARAD seeks comments from interested parties as to any effect this action may have on U.S. vessel builders or businesses in the U.S. that use U.S.-flag vessels. Information about the requestor’s vessel, including a brief description of the proposed service, is listed below.

DATES: Submit comments on or before May 6, 2024.

ADDRESSES: You may submit comments identified by DOT Docket Number MARAD–2024–0048 by any one of the following methods:

- *Federal eRulemaking Portal:* Go to <https://www.regulations.gov>. Search MARAD–2024–0048 and follow the instructions for submitting comments.
- *Mail or Hand Delivery:* Docket Management Facility is in the West Building, Ground Floor of the U.S. Department of Transportation. The Docket Management Facility location address is U.S. Department of Transportation, MARAD–2024–0048, 1200 New Jersey Avenue SE, West Building, Room W12–140, Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except on Federal holidays.

Note: If you mail or hand-deliver your comments, we recommend that you include your name and a mailing address, an email address, or a telephone number in the body of your document so that we can contact you if we have questions regarding your submission.

Instructions: All submissions received must include the agency name and specific docket number. All comments received will be posted without change to the docket at www.regulations.gov, including any personal information provided. For detailed instructions on submitting comments, or to submit comments that are confidential in nature, see the section entitled Public Participation.

FOR FURTHER INFORMATION CONTACT:

Patricia Hagerty, U.S. Department of Transportation, Maritime Administration, 1200 New Jersey Avenue SE, Room W23–461, Washington, DC 20590. Telephone: (202) 366–0903. Email: patricia.hagerty@dot.gov.

SUPPLEMENTARY INFORMATION: As described in the application, the intended service of the vessel ICHTHYS is:

Intended Commercial Use of Vessel: Requester intends to offer sightseeing and birdwatching tours around Kodiak Island.

Geographic Region Including Base of Operations: Alaska. Base of Operations: Kodiak, Alaska.

Vessel Length and Type: 33’ motor.

The complete application is available for review identified in the DOT docket as MARAD 2024–0048 at <https://www.regulations.gov>. Interested parties may comment on the effect this action may have on U.S. vessel builders or businesses in the U.S. that use U.S.-flag vessels. If MARAD determines, in accordance with 46 U.S.C. 12121 and MARAD’s regulations at 46 CFR part 388, that the employment of the vessel in the coastwise trade to carry no more than 12 passengers will have an unduly adverse effect on a U.S.-vessel builder or a business that uses U.S.-flag vessels in that business, MARAD will not issue an approval of the vessel’s coastwise endorsement eligibility. Comments should refer to the vessel name, state the commenter’s interest in the application, and address the eligibility criteria given in section 388.4 of MARAD’s regulations at 46 CFR part 388.

Public Participation*How do I submit comments?*

Please submit your comments, including the attachments, following the instructions provided under the above heading entitled **ADDRESSES**. Be advised that it may take a few hours or even days for your comment to be reflected on the docket. In addition, your comments must be written in English. We encourage you to provide concise comments and you may attach additional documents as necessary. There is no limit on the length of the attachments.

Where do I go to read public comments, and find supporting information?

Go to the docket online at <https://www.regulations.gov>, keyword search MARAD–2024–0048 or visit the Docket Management Facility (see **ADDRESSES** for hours of operation). We recommend that you periodically check the Docket for new submissions and supporting material.

Will my comments be made available to the public?

Yes. Be aware that your entire comment, including your personal identifying information, will be made publicly available.

May I submit comments confidentially?

If you wish to submit comments under a claim of confidentiality, you should submit the information you claim to be confidential commercial information by email to SmallVessels@dot.gov. Include in the email subject heading “Contains Confidential Commercial Information” or “Contains CCI” and state in your submission, with specificity, the basis for any such

confidential claim highlighting or denoting the CCI portions. If possible, please provide a summary of your submission that can be made available to the public.

In the event MARAD receives a Freedom of Information Act (FOIA) request for the information, procedures described in the Department's FOIA regulation at 49 CFR 7.29 will be followed. Only information that is ultimately determined to be confidential under those procedures will be exempt from disclosure under FOIA.

Privacy Act

Anyone can search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). For information on DOT's compliance with the Privacy Act, please visit <https://www.transportation.gov/privacy>.

(Authority: 49 CFR 1.93(a), 46 U.S.C. 55103, 46 U.S.C. 12121)

By Order of the Maritime Administrator,
T. Mitchell Hudson, Jr.,
Secretary, Maritime Administration.

[FR Doc. 2024-07143 Filed 4-3-24; 8:45 am]

BILLING CODE 4910-81-P

DEPARTMENT OF TRANSPORTATION

Office of the Secretary

[Docket No. DOT-OST-2023-0063]

Agency Information Collection Activities: Approval of Information Collection

AGENCY: Office of the Secretary (OST), DOT.

ACTION: 30-Day notice and request for comments.

SUMMARY: The proposed information collection request (ICR) renewal described below will be submitted to the Office of Management and Budget (OMB) for review and approval, as required by the Paperwork Reduction Act of 1995 (PRA). The Department of Transportation (DOT) is soliciting public comments on this proposed collection renewal. The collection is necessary for administration of the Multimodal Project Discretionary Grants (MPDG). This includes three funding opportunities: the "National Infrastructure Project Assistance grants program (Mega)," the "Nationally Significant Multimodal Freight and Highways Projects grants program (INFRA)," and the "Rural Surface

Transportation Grant program (Rural)". The MPDG provides Federal financial assistance for surface transportation infrastructure projects—including highway and bridge, intercity passenger rail, railway-highway grade and separation, wildlife crossing, public transportation, marine highway, and freight and multimodal projects, or groups of such projects, of national or regional significance, as well as to projects to improve and expand the surface transportation infrastructure in rural areas. The DOT on its own made additional changes to update time and estimated costs. Additionally, DOT removed the program evaluation stage (survey) and will submit that separately if conducted.

DATES: Written comments should be submitted by May 6, 2024.

ADDRESSES: To ensure that you do not duplicate your docket submissions, please submit them by only one of the following means:

- *Federal eRulemaking Portal:* Go to <http://www.regulations.gov> and follow the online instructions for submitting comments.
- *Mail:* Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Ave. SE, West Building Ground Floor, Room W12-140, Washington, DC 20590-0001.
- *Hand Delivery:* West Building Ground Floor, Room W-12-140, 1200 New Jersey Ave. SE, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-366-9329.

Instructions: To ensure proper docketing of your comment, please include the agency name and docket number [DOT-OST-2023-0063] at the beginning of your comments. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

FOR FURTHER INFORMATION CONTACT: For further information regarding this notice, please contact the Office of the Secretary via email at MPDGgrants@dot.gov, or call Paul Baumer at (202) 366-1092. A TDD is available for individuals who are deaf or hard of hearing at 202-366-3993.

SUPPLEMENTARY INFORMATION: New Collection. OMB number will be issued after the collection is approved.

Title: Multimodal Project Discretionary Grant (MPDG).

Form Numbers: None.

Type of Review: New Information Collection Request (ICR).

Background: The Office of the Secretary ("OST") within the Department of Transportation (DOT)

provides financial assistance for surface transportation infrastructure projects—including to highway and bridge, intercity passenger rail, railway-highway grade and separation, wildlife crossing, public transportation, marine highway, and freight and multimodal projects, or groups of such projects, of national or regional significance, as well as to projects to improve and expand the surface transportation infrastructure in rural areas. Infrastructure Investment and Jobs Act (Pub. L. 117-58, November 15, 2021) (Bipartisan Infrastructure Law, or BIL) provided funds to the Department across three programs to invest in projects of national or regional significance—the National Infrastructure Project Assistance grants program, found under 49 U.S.C. 6701 ("Mega"), the Nationally Significant Multimodal Freight and Highways Projects grants program, found at 23 U.S.C. 117 (Infrastructure for Rebuilding America or "INFRA"), and the Rural Surface Transportation Grant program, found at 23 U.S.C. 173 ("Rural"). To help streamline the process for applicants, the Department has combined the applications for the Mega, INFRA, and Rural programs into the MPDG common application.

The Nationally Significant Multimodal Freight and Highways Projects grants program ("INFRA") (23 U.S.C. 117) was established in the Fixing American's Surface Transportation Act of 2015 ("FAST ACT"), Public Law 114-94 § 1105, and continued in the Infrastructure Investment and Jobs Act, Public Law 117-58 (2021). OST is referring to these grants as "FASTLANE" or "INFRA" Discretionary Grants, depending on the year of award.

The Bipartisan Infrastructure Law established two new programs along with the reauthorization of INFRA. The Mega Program, known statutorily as the National Infrastructure Project Assistance program (49 U.S.C. 6701), will support large, complex projects that are difficult to fund by other means and likely to generate national or regional economic, mobility, or safety benefits. The Rural Surface Transportation Grant Program (23 U.S.C. 173) will support projects to improve and expand the surface transportation infrastructure in rural areas to increase connectivity, improve the safety and reliability of the movement of people and freight, and generate regional economic growth and improve quality of life.

The DOT combined these three programs into single Notice of Funding Opportunity (NOFO) to provide a more efficient application process for project sponsors. While they remain separate

programs for the purposes of award, the programs share many common characteristics. Because of these shared characteristics, it is possible for many projects to be eligible and considered for multiple programs using a single application.

This notice seeks comments on the proposed information collection, which will collect information necessary to support the ongoing oversight and administration of previous awards, the evaluation and selection of new applications, and the funding agreement negotiation stage for new awards.

The reporting requirements for the program is as follows:

To be considered to receive a MPDG grant, a project sponsor must submit an application to DOT containing a project narrative, as detailed in the NOFO. The project narrative should include the information necessary for the

Department to determine that the project satisfies eligibility requirements as warranted by law.

Following the announcement of a funding award, the recipient and DOT will negotiate and sign a funding agreement. In the agreement, the recipient must describe the project that DOT agreed to fund, which is the project that was described in the MPDG application or a reduced-scope version of that project. The agreement also includes project schedule milestones, a budget, and project-related climate change and equity planning and policies.

During the project monitoring stage, grantees will submit reports on the financial condition of the project and the project's progress. Grantees will submit progress and monitoring reports to the Government on a quarterly basis until completion of the project. The

progress reports will include an SF-425, Federal Financial Report, and other information determined by the administering DOT Operating Administration. This information will be used to monitor grantees' use of Federal funds, ensuring accountability and financial transparency in the MPDG programs.

For the purposes of estimating the information collection burden below for new applicants and awardees, the Department is assuming that for each year 2023–2025, the Department will review approximately 500 applications in Year 1, negotiate 45 funding agreements in Year 2, and begin quarterly project monitoring for 45 projects in Year 3. For a new applicant in 2023, their burden will be 100 hours in 2023, 6 hours in 2024, and 20 hours in 2025. See Table 1 below:

TABLE 1

Respondent	Year 1 (2023)		Year 2 (2024)		Year 3 (2025)		Total
	Hours	Frequency	Hours	Frequency	Hours	Frequency	
2023 Applicant (500)	100	1	50,000
2023 Awardee (45)	6	1	270
2023 Recipient (45)	5	4	900
2024 Applicant (500)	100	1	50,000
2024 Awardee (45)	6	1	270
2024 Recipient (45)
2025 Applicant (500)	100	1	50,000
2025 Awardee (45)
2025 Recipient (45)

This Notice is separately estimating the information collection burden for projects awarded from 2016–2022. Approximately 60 of these projects are in the project monitoring phase in Year 1, while 47 projects are still negotiating funding agreements. In Year 2,

approximately 30 of these projects will begin project monitoring, while approximately 20 projects will cease reporting once their projects are completed. In Year 3, 10 projects will begin project monitoring while 20 projects will cease reporting. The

individual burden for a project awarded from 2016–2021 will depend on when they were selected, when they completed negotiation of their funding agreement, and when their project reaches completion. See Table 2 below:

TABLE 2

Respondent	Year 1			Year 2			Year 3			Total
	Number	Hrs	Freq	Number	Hrs	Freq	Number	Hrs	Freq	
2016–2022 Awardee	47	4	1	10	4	1	0	4	1	200
2016–2022 Recipient	70	5	4	77	5	4	64	5	4	3,800
2016–2022 Project Closed	0	0	0	20	0	0	43	0	0

The Department's estimated burden for this information collection is the following:

For New Applications:
Expected Number of Respondents: Approximately 500 per year.
Frequency: Once.
Estimated Average Burden per Response: 100 hours for each new Application.

For Funding Agreements:
Expected Number of Respondents: Approximately 45 in Year 1, 2 and 3.
Frequency: Once.
Estimated Average Burden per Response: 6 hours for each new Funding Agreement.
For Project Monitoring:

Expected Number of Respondents: Approximately 47 in Year 1, 93 in Year 2, 130 in Year 3.
Frequency: Quarterly.
Estimated Average Burden per Response: 5 hours for each request for Quarterly Progress and Monitoring Report.
Estimated Total 3-Year Burden on Respondents: 79,700 hours. (New

Applicants [75,000 hrs], New Awardees/ Recipients [700 hrs] + Prior Awardees/ Recipients [4000 hrs]).

The following is detailed information and instructions regarding the specific reporting requirements for each report identified above:

Application Stage

To be considered to receive a MPDG grant, a project sponsor must submit an application to DOT containing a project narrative, as detailed in the NOFO. The project narrative should include the information necessary for the Department to determine that the project satisfies eligibility requirements.

Applications must be submitted through www.Grants.gov. Instructions for submitting applications can be found at <https://www.transportation.gov/grants/mpdg-how-apply>. The application must include the Standard Form 424 (Application for Federal Assistance), Standard Form 424C (Budget Information for Construction Programs), cover page, and the Project Narrative.

The application should include a table of contents, maps, and graphics, as appropriate, to make the information easier to review. The Department recommends that the application be prepared with standard formatting preferences (*i.e.*, a single-spaced document, using a standard 12-point font such as Times New Roman, with 1-inch margins). The project narrative may not exceed 25 pages in length, excluding cover pages and table of contents. The only substantive portions that may exceed the 25-page limit are documents supporting assertions or conclusions made in the 25-page project narrative. If possible, website links to supporting documentation should be provided rather than copies of these supporting materials. If supporting documents are submitted, applicants should clearly identify within the project narrative the relevant portion of the project narrative that each supporting document supports. At the applicant's discretion, relevant materials provided previously to a modal administration in support of a different USDOT financial assistance program may be referenced and described as unchanged.

OST estimates that it takes approximately 100 person-hours to compile an application package for a MPDG application. Since OST expects to receive 500 applications per funding

round, the total hours required are estimated to be 50,00 hours (100 hours × 500 applications = 50,000 hours) on a one-time basis, per funding round.

Funding Agreement Stage

DOT enters a funding agreement with each recipient. In the agreement, the recipient describes the project that DOT agreed to fund, which is typically the project that was described in the MPDG application or a reduced-scope version of that project. The agreement also includes a project schedule, budget, and project related climate change and equity planning and policies.

OST estimates that it takes approximately 6 person-hours to respond to provide the information necessary for funding agreements. Based on previous rounds of MPDG awards, OST estimates that there will likely be 45 agreements negotiated per additional funding round. The total hours required are estimated to be 270 (6 hours × 45 agreements = 270 hours) on a one-time basis, per funding round.

Project Monitoring Stage

OST requires each recipient to submit quarterly reports during the project to ensure the proper and timely expenditure of Federal funds under the grant.

The requirements comply with 2 CFR part 200 and are restated in the funding agreement. During the project monitoring stage, the grantee will complete Quarterly Progress Reports to allow DOT to monitor the project budget and schedule.

OST estimates that it takes approximately 5 person-hours to develop and submit a quarterly progress report. OST expects approximately 45 projects to be awarded per funding round, while grants awarded in prior years will reach completion during the year and would no longer need to submit these reports. OST expects recipients and awardees from 2016–2021 will require 3800 hours to submit project monitoring reports while new recipients and awardees will require 900 hours from 2023–2025.

Authority: The Paperwork Reduction Act of 1995; 44 U.S.C. Chapter 35, as amended; and 49 CFR 1.48.

John Augustine,

Director of the Office of Infrastructure Finance and Innovation, Office of the Under Secretary for Transportation Policy.

[FR Doc. 2024-07055 Filed 4-3-24; 8:45 am]

BILLING CODE 4910-9X-P

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

Notice of OFAC Sanctions Actions

AGENCY: Office of Foreign Assets Control, Treasury.

ACTION: Notice.

SUMMARY: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing the names of one or more persons that have been placed on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) based on OFAC's determination that one or more applicable legal criteria were satisfied. All property and interests in property subject to U.S. jurisdiction of these persons are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.

DATES: See **SUPPLEMENTARY INFORMATION** section for effective date(s).

FOR FURTHER INFORMATION CONTACT: OFAC: Bradley T. Smith, Director, tel.: 202-622-2490; Associate Director for Global Targeting, tel.: 202-622-2420; Assistant Director for Licensing, tel.: 202-622-2480; Assistant Director for Regulatory Affairs, tel.: 202-622-4855; or the Assistant Director for Sanctions Compliance & Evaluation, tel.: 202-622-2490.

SUPPLEMENTARY INFORMATION:

Electronic Availability

The SDN List and additional information concerning OFAC sanctions programs are available on OFAC's website (<https://www.treasury.gov/ofac>).

Notice of OFAC Action[s]

On March 25, 2024, OFAC determined that the property and interests in property subject to U.S. jurisdiction of the following persons are blocked under the relevant sanctions authorities listed below.

BILLING CODE 4810-AL-P

Individuals:

1. BUKANOV, Timur Evgenyevich (Cyrillic: БУКАНОВ, Тимур Евгеньевич) (a.k.a. BUKANOV, Timur Evgen'evich; a.k.a. BUKANOV, Timur Evgenevich), Apt. 103, Vilisa Lazisa Street 41, Moscow, Russia; DOB 03 Aug 1978; nationality Russia; citizen Russia; Email Address timur.bukanov@gmail.com; Gender Male; Tax ID No. 773312065789 (Russia) (individual) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of Executive Order 14024 of April 15, 2021, "Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation" 86 FR 20249, 3 CFR, 2021 Comp., p. 542 (Apr. 15, 2021) (E.O. 14024), for operating or having operated in the financial services sector of the Russian Federation economy.

2. КАЙГОРОДОВ, Igor Veniaminovich (Cyrillic: КАЙГОРОДОВ, Игорь Вениаминович), Izhevsk, Russia; DOB 29 Nov 1974; nationality Russia; citizen Russia; Gender Male; Tax ID No. 183475635611 (Russia); Russian State Individual Business Registration Number Pattern (OGRNIP) 315183100004295 (Russia) (individual) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy.

Entities:

1. BITFINGROUP OU (Latin: BITFINGROUP OÜ), Lasnamae linnaosa, Vaike-Paala tn 2, Tallinn, Harju maakond 11415, Estonia; Organization Established Date 23 Sep 2021; Registration Number 16323700 (Estonia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(vii) of E.O. 14024 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Timur Evgenyevich BUKANOV, a person whose property and interests are blocked pursuant to E.O. 14024.

2. OBSHCHESTVO S OGRANICHENNOY OTVETSTVENNOSTYU TSENTR OBRABOTKI ELEKTRONNYKH PLATEZHEY (Cyrillic: ООО ЦЕНТР ОБРАБОТКИ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ) (a.k.a. NETEX TRADE; a.k.a. NETEX24; a.k.a. OBSHCHESTVO S OGRANICHENNOJ OTVETSTVENNOSTYU CENTR OBRABOTKI ELEKTRONNYKH PLATEZHEJ; a.k.a. OBSHCHESTVO S OGRANICHENNOY OTVETSTVENNOSTYU TSENTR OBRABOTKI ELEKTRONNYKH PLATEZHEI; a.k.a. "LIMITED LIABILITY COMPANY CENTER FOR PROCESSING ELECTRONIC PAYMENTS"; a.k.a. "NETEXCHANGE"; a.k.a. "ООО ТСОЕР" (Cyrillic: "ООО ЦОЭП")), Ul. Vilisa Latsisa D. 41, KV. 103, Moscow 125480, Russia; Business Center Iskra-Park, 35, Leningradsky Prospect, Moscow,

Russia; Website <https://www.netex24.net>; alt. Website <https://www.netex24.com>; alt. Website <https://www.netex.trade>; alt. Website <https://www.netexchange.ru>; Organization Established Date 28 Feb 2014; Tax ID No. 7733872485 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the financial services sector of the Russian Federation economy.

3. JOINT-STOCK COMPANY B-CRYPTO (Cyrillic: АКЦИОНЕРНОЕ ОБЩЕСТВО Б-КРИПТО) (a.k.a. AKTSIONERNOYE OBSHCHESTVO B-KRIPTO), Ter. Skolkovo Innovatsionnogo Tsentra, B-R Bolshoi, D. 42, Str. 1, Pomeshch. #1160, Moscow 121205, Russia; Website <https://www.b-crypto.ru>; Organization Established Date 12 Oct 2022; Tax ID No. 9731101346 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the financial services sector of the Russian Federation economy.

4. OBSHCHESTVO S OGRANICHENNOY OTVETSTVENNOSTYU ATOMAIZ (Cyrillic: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ АТОМАЙЗ) (a.k.a. ATOMYZE; a.k.a. ATOMYZE RUSSIA; a.k.a. LIMITED LIABILITY COMPANY ATOMAYZ), Nab. Presnenskaya D. 12, Pomeshch. 2/59, Moscow 123112, Russia; Website <https://www.atomyze.ru>; Organization Established Date 12 Nov 2020; Tax ID No. 9703021466 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the financial services sector of the Russian Federation economy.

5. OBSHCHESTVO S OGRANICHENNOY OTVETSTVENNOSTYU LAITKHAUS (Cyrillic: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ ЛАЙТХАУС) (a.k.a. "LIGHTHOUSE"), Pr-Kt Vernadskogo D. 53, Floor/Pomeshch. 3/I, Kom. 37, Moscow 119415, Russia; Organization Established Date 05 Jul 2017; Tax ID No. 9723031631 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the financial services sector of the Russian Federation economy.

6. OBSHCHESTVO S OGRANICHENNOY OTVETSTVENNOSTYU SISTEMY RASPREDELENNOGO REYESTRA (Cyrillic: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ СИСТЕМЫ РАСПРЕДЕЛЕННОГО РЕЕСТРА) (a.k.a. DISTRIBUTED LEDGER SYSTEMS LLC; a.k.a. LIMITED LIABILITY COMPANY DISTRIBUTED LEDGER TECHNOLOGY; a.k.a. "DISTRIBUTED REGISTRY SYSTEMS"; a.k.a. "MASTERCHAIN"), Ul. Kompozitorskaya D. 17, Et./Pom. 7/I, Kom. 11-17, Moscow 121099, Russia; Website <https://www.masterchain.ru>; Organization Established Date 04 May 2021; Tax ID No. 9704063885 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the financial services sector of the Russian Federation economy.

7. OBSHCHESTVO S OGRANICHENNOY OTVETSTVENNOSTYU WEB3 INTEGRATOR (Cyrillic: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ ВЕБ3 ИНТЕГРАТОР) (a.k.a. "ООО WEB3 INTEGRATOR"), Nab. Bersenevskaya D. 6., Str. 3, Pomeshch. I, Kom 9 Ach, Et 4,

Moscow 119072, Russia; Organization Established Date 15 Jan 2019; Tax ID No. 7706464945 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy.

8. OBSHCHESTVO S OGRANICHENNOY OTVETSTVENNOSTYU WEB3 TEKHOLOGII (Cyrillic: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ ВЕБ3 ТЕХНОЛОГИИ) (a.k.a. “LIMITED LIABILITY COMPANY WEB3 TECHNOLOGIES” (Cyrillic: “ООО ВЕЙБ3”); a.k.a. “WEB3 TECH”; a.k.a. “WEB3 TECHNOLOGY LLC”), Nab. Bersenevskaya D. 6, Str 3, Et 4 Pom.I Kom 9, Moscow 119072, Russia; Website <https://www.web3tech.ru>; Organization Established Date 11 Aug 2017; Tax ID No. 7724417440 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy.

9. TOKENTRUST HOLDINGS LIMITED (Cyrillic: ТОКЕНТРАСТ ХОЛДИНГЗ ЛИМИТЕД), Lara Court, Arch. Makariou Iii 276, Limassol, Cyprus; Organization Established Date 11 Jun 2020; Registration Number HE410067 (Cyprus) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the financial services sector of the Russian Federation economy.

10. BITPAPA IC FZC LLC (Arabic: بيتابا اي سي ش.م.ح /ذ.م.م) (a.k.a. BITPAPA; a.k.a. BITPAPA FZC LLC (Arabic: بيت بابا ش.م.ح/ذ.م.م); a.k.a. BITPAPA PAY; a.k.a. PAPA HOLDING LTD), A-0059-652 Flamingo Villas, Ajman Media City Free Zone, Ajman, United Arab Emirates; Website <https://www.bitpapa.com>; alt. Website <https://www.bitpapa.org>; Organization Established Date 29 Apr 2022; Registration Number 5069 (United Arab Emirates); alt. Registration Number RA000693_172229 (Belize); Economic Register Number (CBLS) 11874154 (United Arab Emirates) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the financial services sector of the Russian Federation economy

11. CRYPTO EXPLORER DMCC (Arabic: كريبتو إكسپلورر د.م.س; Cyrillic: КРИПТО ЭКСПЛОРЕР ДМСИСИ) (a.k.a. AWEX CRYPTO EXPLORER DMCC; a.k.a. “AWEX”; a.k.a. “BANKOFF”), 12 Presnenskaya Embankment (Federation Tower), Moscow City, Moscow 123317, Russia; 612 Gold Crest Executive Tower, Jumeirah Lake Towers, Dubai, United Arab Emirates; Website <https://www.awex.pro>; Organization Established Date 09 Aug 2023; Registration Certificate Number (Dubai) DMCC193946 (United Arab Emirates); License DMCC-852167 (United Arab Emirates); Economic Register Number (CBLS) 11934635 (United Arab Emirates) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the financial services sector of the Russian Federation economy

12. OBSHCHESTVO S OGRANICHENNOY OTVETSTVENNOSTYU KRIPTO EKSPLOREER (Cyrillic: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

КРИПТО ЭКСПЛОРЕР) (a.k.a. LIMITED LIABILITY COMPANY CRYPTO EXPLORER), Ul. Karla Marksa D. 13A, K. 1, Pomeshch. 43, Ulyanovsk 432071, Russia; Organization Established Date 13 Oct 2022; Tax ID No. 7300009215 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(vii) of E.O. 14024 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, CRYPTO EXPLORER DMCC, a person whose property and interests are blocked pursuant to E.O. 14024.

13. AUTONOMOUS NON-PROFIT ORGANIZATION OF ADDITIONAL PROFESSIONAL EDUCATION ECHELON TRAINING CENTER (Cyrillic: АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ УЧЕБНЫЙ ЦЕНТР ЭШЕЛОН) (a.k.a. AVTONOMNAYA NEKOMMERCHESKAYA ORGANIZATSIYA DOPOLNITELNOGO PROFESSIONALNOGO OBRAZOVANIYA UCHEBNIYI TSENTR ESHELON; a.k.a. UCHEBNIYI TSENTR ESHELON, ANO), Ul. Elektrozavodskaya d. 24, str. 1, Moscow 107023, Russia; Organization Established Date 23 Oct 2008; Tax ID No. 7718271218 (Russia); Registration Number 1087799033519 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy.

14. JOINT STOCK COMPANY ECHELON TECHNOLOGIES (Cyrillic: АКЦИОНЕРНОЕ ОБЩЕСТВО ЭШЕЛОН ТЕХНОЛОГИИ) (a.k.a. AKTSIONERNOE OBSHESTVO ESHELON TEKHNologii; a.k.a. AO ECHELON TECHNOLOGIES; a.k.a. JSC ECHELON TECHNOLOGIES), Ul. Elektrozavodskaya d. 24 Office 24, Moscow 107023, Russia; Organization Established Date 06 Sep 2011; Tax ID No. 7718859120 (Russia); Registration Number 1117746703480 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy.

15. LIMITED LIABILITY COMPANY CYBERSECURITY LABORATORY (Cyrillic: ЛАБОРАТОРИЯ КИБЕРБЕЗОПАСНОСТИ), Ul. Gorkogo d. 9, Office KH2-KH5, Floor 2, Sevastopol 299001, Ukraine; Organization Established Date 24 Nov 2015; Tax ID No. 9204558128 (Russia); Registration Number 1159204030358 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(vii) of E.O. 14024 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, JOINT STOCK COMPANY ECHELON UNION FOR SCIENCE AND DEVELOPMENT, a person whose property and interests are blocked pursuant to E.O. 14024.

16. LIMITED LIABILITY COMPANY ECHELON INNOVATIONS (Cyrillic: ЭШЕЛОН ИННОВАЦИИ) (a.k.a. ESHELON INNOVATSII; a.k.a. LLC ECHELON INNOVATIONS), Ul. Elektrozavodskaya d. 24, Moscow 107023, Russia; Organization Established Date 29 Aug 2013; Tax ID No. 7718945192 (Russia); Registration Number 1137746780490 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(vii) of E.O. 14024 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, JOINT STOCK COMPANY ECHELON UNION FOR SCIENCE AND DEVELOPMENT, a person whose property and interests are blocked pursuant to E.O. 14024.

17. LIMITED LIABILITY COMPANY KEY INFORMATION SYSTEMS (Cyrillic: КЛЮЧЕВЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ) (a.k.a. KLYUCHEVYE INFORMATSIONNYE SISTEMY), Ul. Elektrozavodskaya d. 24, Moscow 107023, Russia; Organization Established Date 23 Jul 2014; Tax ID No. 7718990822 (Russia); Registration Number 1147746835830 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(i) of E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy.

18. LIMITED LIABILITY COMPANY PROJECT CONSULTING BUREAU ECHELON (Cyrillic: ПРОЕКТНО-КОНСАЛТИНГОВОЕ БЮРО ЭШЕЛОН) (a.k.a. LLC PKB ECHELON; a.k.a. PROEKTNO-KONSALTINGOVOE BYURO ESHELON), Ul. Elektrozavodskaya d. 24, Moscow 107023, Russia; Organization Established Date 24 Jul 2014; Tax ID No. 7718990935 (Russia); Registration Number 1147746837677 (Russia) [RUSSIA-EO14024].

Designated pursuant to section 1(a)(vii) of E.O. 14024 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, JOINT STOCK COMPANY ECHELON UNION FOR SCIENCE AND DEVELOPMENT, a person whose property and interests are blocked pursuant to E.O. 14024.

Dated: March 25, 2024.

Bradley T. Smith,

*Director, Office of Foreign Assets Control,
U.S. Department of the Treasury.*

[FR Doc. 2024-07159 Filed 4-3-24; 8:45 am]

BILLING CODE 4810-AL-C

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

Notice of OFAC Sanctions Action

AGENCY: Office of Foreign Assets Control, Treasury.

ACTION: Notice.

SUMMARY: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing the names

of three entities and two individuals that have been placed on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) based on OFAC's determination that one or more applicable legal criteria were satisfied. All property and interests in property subject to U.S. jurisdiction of these entities and these individuals are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.

DATES: See **SUPPLEMENTARY INFORMATION** section for effective date(s).

FOR FURTHER INFORMATION CONTACT: OFAC: Bradley T. Smith, Director, tel.: 202-622-2490; Associate Director for Global Targeting, tel.: 202-622-2420; Assistant Director for Licensing, tel.: 202-622-2480; Assistant Director for

Regulatory Affairs, tel.: 202-622-4855; or the Assistant Director for Compliance, tel.: 202-622-2490.

SUPPLEMENTARY INFORMATION:

Electronic Availability

The SDN List and additional information concerning OFAC sanctions programs are available on OFAC's website (<https://ofac.treasury.gov/>).

Notice of OFAC Action

On March 27, 2024, OFAC determined that the property and interests in property subject to U.S. jurisdiction of the following entities and individuals are blocked under the relevant sanctions authority listed below.

BILLING CODE 4810-AL-P

Entities:

1. GAZA NOW (Arabic: غزة الآن) (a.k.a. "GAZAALAN"; a.k.a. "GAZAALANNET"; a.k.a. "GNNANOW"), Gaza; Digital Currency Address - XBT 3Q8H2ZWMtc4R1M3mkmhnTjCoYKTeCFigDP; Digital Currency Address - ETH 0xE950DC316b836e4EeFb8308bf32Bf7C72a1358FF; alt. Digital Currency Address - ETH 0x21B8d56BDA776bbE68655A16895afd96F5534feD; Secondary sanctions risk: section 1(b) of Executive Order 13224, as amended by Executive Order 13886; Organization Established Date 01 May 2012; Digital Currency Address - USDT TTgcTTNbNuFdbhrhvjMZVrdU5KALyzDaPw; alt. Digital Currency Address - USDT TGJvc32ig2u8tQsYMLE7KXHT5NDQroaVNU; alt. Digital Currency Address - USDT TXEsK1sEsKjZ1xtHitnyAAoqw3WLdYdRNW; alt. Digital Currency Address - USDT TH96tFMn8KGiYSLiwcV3E2UiaJc8jmcbz3; alt. Digital Currency Address - USDT 0x175d44451403Edf28469dF03A9280c1197ADb92c [SDGT] (Linked To: HAMAS; Linked To: AYASH, Mustafa).

Designated pursuant to section 1(a)(iii)(C) of Executive Order 13224 of September 23, 2001, "Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism," 66 FR 49079, as amended by Executive Order 13886 of September 9, 2019, "Modernizing Sanctions To Combat Terrorism," 84 FR 48041 (E.O. 13224, as amended), for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or service to or in support of, HAMAS, a person whose property and interests in property are blocked pursuant to E.O. 13224, as amended.

2. AL-QURESHI EXECUTIVES, 4 Culham Court, Redford Way, Uxbridge, London UB8 1SY, United Kingdom; Secondary sanctions risk: section 1(b) of Executive Order 13224, as amended by Executive Order 13886; Organization Established Date 20 Dec 2021; Organization Type: Other business support service activities n.e.c.; Company Number 13808616 (United Kingdom) [SDGT] (Linked To: SULTANA, Aozma).

Designated pursuant to section 1(a)(iii)(A) of E.O. 13224, as amended, for being owned, controlled, or directed by, or having acted or purported to act for or on behalf of, directly or indirectly, Aozma Sultana, a person whose property and interests in property are blocked pursuant to section 1(a)(iii)(C) of E.O. 13224, as amended.

3. AAKHIRAH LIMITED, 4 Culham Court, Redford Way, Uxbridge, London UB8 1SY, United Kingdom; Secondary sanctions risk: section 1(b) of Executive Order 13224, as amended by Executive Order 13886; Organization Established Date 18 Mar 2009; Organization Type: Other business support service activities n.e.c.; Company Number 06850415 (United Kingdom) [SDGT] (Linked To: SULTANA, Aozma).

Designated pursuant to section 1(a)(iii)(A) of E.O. 13224, as amended, for being owned, controlled, or directed by, or having acted or purported to act for or on behalf of, directly or indirectly, Aozma Sultana, a person whose property and interests in property are blocked pursuant to section 1(a)(iii)(C) of E.O. 13224, as amended.

Individuals:

1. AYASH, Mustafa (a.k.a. AYASH, Mostafa Moin Mahmoud; a.k.a. AYYASH, Mustafa), Wienerstrasse 20, Linz 4020, Austria; DOB 18 Sep 1992; POB Gaza Strip; nationality Palestinian; Gender Male; Secondary sanctions risk: section 1(b) of Executive Order 13224, as amended by Executive Order 13886; Passport K1332951 (Austria) issued 17 Dec 2018 expires 16 Dec 2023; National ID No. 160715450005 (Austria) issued 04 Dec 2018 (individual) [SDGT] (Linked To: GAZA NOW).

Designated pursuant to section 1(a)(iii)(B) E.O. 13224, as amended, for owning or controlling, directly or indirectly, Gaza Now, a person whose property and interest in property are blocked pursuant to section 1(a)(iii)(C) of E.O. 13224, as amended.

2. SULTANA, Aozma (a.k.a. QURESHI, Aozma), 4 Culham Court, Redford Way, Uxbridge, London UB8 1SY, United Kingdom; 5 Maryport Road, Luton, Bedfordshire LU4 8EA, United Kingdom; 8 St. Mildreds Avenue, Luton, Bedfordshire LU31QR, United Kingdom; DOB 30 Oct 1982; POB Luton, UK; nationality United Kingdom; Gender Female; Secondary sanctions risk: section 1(b) of Executive Order 13224, as amended by Executive Order 13886; Passport 523632616 (United Kingdom) (individual) [SDGT] (Linked To: AL-QURESHI EXECUTIVES; Linked To: AAKHIRAH LIMITED).

Designated pursuant to section 1(a)(iii)(C) of E.O. 13224, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, Gaza Now, a person whose property and interests in property are blocked pursuant to section 1(a)(i) of E.O. 13224, as amended.

Dated: March 27, 2024.

Bradley T. Smith,

*Director, Office of Foreign Assets Control,
U.S. Department of the Treasury.*

[FR Doc. 2024-07160 Filed 4-3-24; 8:45 am]

BILLING CODE 4810-AL-C

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

Notice of OFAC Sanctions Action

AGENCY: Office of Foreign Assets Control, Treasury.

ACTION: Notice.

SUMMARY: The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing the names of one entity and two individuals that

have been placed on OFAC's Specially Designated Nationals and Blocked Persons List based on OFAC's determination that one or more applicable legal criteria were satisfied. All property and interests in property subject to U.S. jurisdiction of this entity and these individuals are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.

DATES: See **SUPPLEMENTARY INFORMATION** section for effective date(s).

FOR FURTHER INFORMATION CONTACT: OFAC: Bradley T. Smith, Director, tel.: 202-622-2490; Associate Director for Global Targeting, tel.: 202-622-2420; Assistant Director for Licensing, tel.: 202-622-2480; Assistant Director for Regulatory Affairs, tel.: 202-622-4855;

or the Assistant Director for Compliance, tel.: 202-622-2490.

SUPPLEMENTARY INFORMATION:

Electronic Availability

The Specially Designated Nationals and Blocked Persons List and additional information concerning OFAC sanctions programs are available on OFAC's website (<https://ofac.treasury.gov/>).

Notice of OFAC Action

On March 25, 2024, OFAC determined that the property and interests in property subject to U.S. jurisdiction of the following entity and individuals are blocked under the relevant sanctions authorities listed below.

BILLING CODE 4810-AL-P

Entity:

1. WUHAN XIAORUIZHI SCIENCE AND TECHNOLOGY COMPANY, LIMITED (Chinese Simplified: 武汉晓睿智科技有限责任公司), 2nd Floor, No. 16, Huashiyuan North Road, East Lake New Technology Development Zone, Wuhan, Hubei Province, China; Organization Established Date 08 Mar 2010; Organization Type: Computer programming activities; Unified Social Credit Code (USCC) 91420100551956105K (China) [CYBER2].

Designated pursuant to section 1(a)(ii) of Executive Order 13694 of April 1, 2015, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," 80 FR 18077, 3 CFR, 2015 Comp., p. 297, as amended by Executive Order 13757 of December 28, 2016, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," 82 FR 1, 3 CFR, 2016 Comp., p. 659 (E.O. 13694, as amended) for being responsible for or complicit in, or having engaged in, directly or indirectly, an activity described in section 1(a)(ii)(A) of E.O. 13694, as amended.

Individuals:

1. ZHAO, Guangzong (Chinese Simplified: 赵光宗), Hubei Province, China; DOB 12 Nov 1985; POB Jingzhou Municipality, China; nationality China; citizen China; Gender Male; National ID No. 421003198511121539 (China) (individual) [CYBER2].

Designated pursuant to section 1(a)(iii)(C) of E.O. 13694, as amended for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interest in property are blocked pursuant to E.O. 13694, as amended.

2. NI, Gaobin (Chinese Simplified: 倪高彬), Hubei Province, China; DOB 27 Oct 1985; POB Jingzhou Municipality, China; nationality China; citizen China; Gender Male; National ID No. 421003198510272917 (China) (individual) [CYBER2].

Designated pursuant to section 1(a)(iii)(C) of E.O. 13694, as amended for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interest in property are blocked pursuant to E.O. 13694, as amended.

Dated: March 25, 2024.

Bradley T. Smith,

*Director, Office of Foreign Assets Control,
U.S. Department of the Treasury.*

[FR Doc. 2024-07161 Filed 4-3-24; 8:45 am]

BILLING CODE 4810-AL-C

DEPARTMENT OF THE TREASURY**Interest Rate Paid on Cash Deposited To Secure U.S. Immigration and Customs Enforcement Immigration Bonds**

AGENCY: Departmental Offices, Treasury.

ACTION: Notice.

SUMMARY: For the period beginning April 1, 2024, and ending on June 30, 2024, the U.S. Immigration and Customs Enforcement Immigration Bond interest rate is 3 per centum per annum.

DATES: Rates are applicable April 1, 2024, to June 30, 2024.

ADDRESSES: Comments or inquiries may be mailed to Will Walcutt, Supervisor, Funds Management Branch, Funds Management Division, Fiscal Accounting, Bureau of the Fiscal Services, Parkersburg, West Virginia 26106-1328.

You can download this notice at the following internet addresses: <<http://www.treasury.gov>> or <<http://www.federalregister.gov>>.

FOR FURTHER INFORMATION CONTACT: Ryan Hanna, Manager, Funds

Management Branch, Funds Management Division, Fiscal Accounting, Bureau of the Fiscal Service, Parkersburg, West Virginia 261006-1328 (304) 480-5120; Will Walcutt, Supervisor, Funds Management Branch, Funds Management Division, Fiscal Accounting, Bureau of the Fiscal Services, Parkersburg, West Virginia 26106-1328, (304) 480-5117.

SUPPLEMENTARY INFORMATION: Federal law requires that interest payments on cash deposited to secure immigration bonds shall be “at a rate determined by the Secretary of the Treasury, except that in no case shall the interest rate exceed 3 per centum per annum.” 8 U.S.C. 1363(a). Related Federal regulations state that “Interest on cash deposited to secure immigration bonds will be at the rate as determined by the Secretary of the Treasury, but in no case will exceed 3 per centum per annum or be less than zero.” 8 CFR 293.2. Treasury has determined that interest on the bonds will vary quarterly and will accrue during each calendar quarter at a rate equal to the lesser of the average of the bond equivalent rates on 91-day Treasury bills auctioned during the preceding calendar quarter, or 3 per centum per annum, but in no case less than zero. [FR Doc. 2015-18545]. In addition to this Notice, Treasury posts the current quarterly rate in Table 2b—Interest Rates for Specific Legislation on the Treasury Direct website.

The Deputy Assistant Secretary for Public Finance, Gary Grippo, having reviewed and approved this document, is delegating the authority to electronically sign this document to Heidi Cohen, Federal Register Liaison for the Department, for purposes of publication in the **Federal Register**.

Heidi Cohen,

Federal Register Liaison.

[FR Doc. 2024-07154 Filed 4-3-24; 8:45 am]

BILLING CODE 4810-25-P

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Notice of Open Public Hearing

AGENCY: U.S.-China Economic and Security Review Commission.

ACTION: Notice of open public hearing.

SUMMARY: Notice is hereby given of the following hearing of the U.S.-China Economic and Security Review Commission. The Commission is mandated by Congress to monitor, investigate, and report to Congress annually on “the national security

implications of the economic relationship between the United States and the People’s Republic of China.” Pursuant to this mandate, the Commission will hold a public hearing in Washington, DC on April 19, 2024 on “China and the Middle East.”

DATES: The hearing is scheduled for Friday, April 19, 2024 at 9:30 a.m.

ADDRESSES: Members of the public will be able to attend in person at a location TBD or view a live webcast via the Commission’s website at www.uscc.gov. Visit the Commission’s website for updates to the hearing location or possible changes to the hearing schedule. Reservations are not required to view the hearing online or in person.

FOR FURTHER INFORMATION CONTACT: Any member of the public seeking further information concerning the hearing should contact Jameson Cunningham, 444 North Capitol Street NW, Suite 602, Washington, DC 20001; telephone: 202-624-1496, or via email at jcunningham@uscc.gov. Reservations are not required to attend the hearing.

ADA Accessibility: For questions about the accessibility of the event or to request an accommodation, please contact Jameson Cunningham via email at jcunningham@uscc.gov. Requests for an accommodation should be made as soon as possible, and at least five business days prior to the event.

SUPPLEMENTARY INFORMATION:

Background: This is the fourth public hearing the Commission will hold during its 2024 reporting cycle. The hearing will begin with an assessment of China’s energy, investment, and economic interests in the Middle East. Next, it will examine China’s diplomatic engagement with Middle Eastern countries and Beijing’s efforts to shape an alternative world order. Finally, it will consider China’s security interests and activities in the Middle East.

The hearing will be co-chaired by Commissioners Aaron Friedberg and Jonathan N. Stivers. Any interested party may file a written statement by April 19, 2024 by transmitting it to the contact above. A portion of the hearing will include a question and answer period between the Commissioners and the witnesses.

Authority: Congress created the U.S.-China Economic and Security Review Commission in 2000 in the National Defense Authorization Act (Pub. L. 106-398), as amended by Division P of the Consolidated Appropriations Resolution, 2003 (Pub. L. 108-7), as amended by Public Law 109-108 (November 22, 2005), as amended by Public Law 113-291 (December 19, 2014).

Dated: March 27, 2024.

Christopher Fioravante,

Director of Operations and Administration, U.S.-China Economic and Security Review Commission.

[FR Doc. 2024-07134 Filed 4-3-24; 8:45 am]

BILLING CODE 1137-00-P

DEPARTMENT OF VETERANS AFFAIRS

[OMB Control No. 2900-0554]

Agency Information Collection Activity: VA Homeless Providers Grant and Per Diem Program

AGENCY: Veterans Health Administration, Department of Veterans Affairs.

ACTION: Notice.

SUMMARY: Veterans Health Administration (VHA), Department of Veterans Affairs (VA), is announcing an opportunity for public comment on the proposed collection of certain information by the agency. Under the Paperwork Reduction Act (PRA) of 1995, Federal agencies are required to publish notice in the **Federal Register** concerning each proposed collection of information, including each proposed extension of a currently approved collection, and allow 60 days for public comment in response to the notice.

DATES: Written comments and recommendations on the proposed collection of information should be received on or before June 3, 2024.

ADDRESSES: Submit written comments on the collection of information through Federal Docket Management System (FDMS) at www.Regulations.gov or to Grant Bennett, Office of Regulations, Appeals, and Policy (10BRAP), Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420 or email to Grant.Bennett@va.gov. Please refer to “OMB Control No. 2900-0554” in any correspondence. During the comment period, comments may be viewed online through FDMS.

FOR FURTHER INFORMATION CONTACT: Dorothy Glasgow, Office of Enterprise and Integration, Data Governance Analytics (008), 810 Vermont Avenue NW, Washington, DC 20420, (202) 461-1084 or email dorothy.glasgow@va.gov. Please refer to “OMB Control No. 2900-0554” in any correspondence.

SUPPLEMENTARY INFORMATION: Under the PRA of 1995, Federal agencies must obtain approval from the Office of Management and Budget (OMB) for each collection of information they conduct or sponsor. This request for comment is

being made pursuant to Section 3506(c)(2)(A) of the PRA.

With respect to the following collection of information, VHA invites comments on: (1) whether the proposed collection of information is necessary for the proper performance of VHA's functions, including whether the information will have practical utility; (2) the accuracy of VHA's estimate of the burden of the proposed collection of information; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or the use of other forms of information technology.

Authority: Public Law 104–13; 44 U.S.C. 3501–3521.

Title: VA Homeless Providers Grant and Per Diem Program.

OMB Control Number: 2900–0554.

Type of Review: Revision of a currently approved collection.

Abstract: Public Law 109–461 provided permanent authority for VA's Homeless Providers Grant and Per Diem (GPD) Program for homeless Veterans. The categories of grants include per diem for non-capital grants, special needs grants, and case management grants. The program will not be awarding capital grants in the coming years. This factor, along with historical program data on the actual number of applications received, has resulted in a decrease in the anticipated number of annual grant applications and associated annual burden hours. There are no changes to the information being collected.

Funds appropriated to the Department of Veterans Affairs (VA) for this program are expected to be significantly less than the total amount requested by applicants. Therefore, information must be collected to determine which applicants are eligible and to prioritize applications for determining who will be awarded funds. VA does not require applicants to use a VA Form to respond to the collection of information. Rather, VA requires applicants to respond to the collection of information as published in the Notice of Funding Opportunity (NOFO) in standard business format, and they may use the Federal-wide Standard Forms from the SF–424 family of forms. VA provides the outline for the collection in the NOFO and uses the standard business format to evaluate applicants for all the grant programs under the statutory authority for VA to make grants.

Affected Public: State, Local, and Tribal Governments.

Estimated Annual Burden: 10,000 hours.

Estimated Average Burden per Respondent: 20 hours.

Frequency of Response: Once annually.

Estimated Number of Respondents: 500.

By direction of the Secretary:

Dorothy Glasgow,

VA PRA Clearance Officer, (Alt.), Office of Enterprise and Integration/Data Governance Analytics, Department of Veterans Affairs.

[FR Doc. 2024–07130 Filed 4–3–24; 8:45 am]

BILLING CODE 8320–01–P

DEPARTMENT OF VETERANS AFFAIRS

Privacy Act of 1974: System of Records

AGENCY: Office of Operations, Security and Preparedness, Department of Veterans Affairs (VA).

ACTION: Notice of a modified system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, notice is hereby given that the Department of Veterans Affairs (VA) is amending the system of records entitled “Police and Security Records—VA” (103VA07B). VA is amending the system of records by updating the following sections: System Name and Number; System Location; System Manager(s); Record Source Categories; Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of Such Uses; Policies and Practice for Storage of Records; Policies and Practices for Retrieval of Records; Policies and Practices for Retention and Disposal of Records; Record Access Procedure; Contesting Procedure; Notification Procedure; History. VA is republishing the system notice in its entirety.

DATES: Comments on this modified system of records must be received no later than May 6, 2024. If no public comment is received during the period allowed for comment or unless otherwise published in the **Federal Register** by VA, the modified system of records will become effective a minimum of 30 days after date of publication in the **Federal Register**. If VA receives public comments, VA shall review the comments to determine whether any changes to the notice are necessary.

ADDRESSES: Comments may be submitted through www.Regulations.gov or mailed to VA Privacy Service, 810 Vermont Avenue NW, (005X6F),

Washington, DC 20420. Comments should indicate that they are submitted in response to “Police and Security Records—VA” (103VA07B). Comments received will be available at regulations.gov for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT:

Edward Dubois, Director, Police Service, 810 Vermont Avenue NW, Washington, DC 20420. Telephone (202) 461–5544 or submit inquiry to OSLE@VA.GOV. The Office of Security and Law Enforcement, Director, Police Service is the system owner and provides the business oversight for this SORN.

SUPPLEMENTARY INFORMATION:

The Office of Security and Law Enforcement oversees the maintenance of law and order and the protection of persons and property on Department property at facilities nationwide. This amended system of records covers Veterans, U.S. Government employees, retirees, volunteers, contractors, subcontractors, or private citizens involved in certain Police Service activities at field facilities and Office of Security and Law Enforcement activities at VA Central Office. Records in the system are maintained electronically and on paper and are retrieved by the name of the individual or personal identifier such as partial or full social security number. The authority to maintain these records is title 38, United States Code (U.S.C.), section 501 and 901–905. The records in this system of records are necessary for the effective administration and management of the Department's nationwide Security and Law Enforcement program. This requires the collection and use of accurate, up-to-date data for the purpose of enforcing the law and protecting persons and property on VA property in accordance with title 38, U.S.C., chapter 9.

Signing Authority

The Senior Agency Official for Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs. Kurt D. DelBene, Assistant Secretary for Information and Technology and Chief Information Officer, approved this document on February 28, 2024 for publication.

Dated: April 1, 2024.

Amy L. Rose,

Government Information Specialist, VA Privacy Service, Office of Compliance, Risk and Remediation, Office of Information and Technology, Department of Veterans Affairs.

SYSTEM NAME AND NUMBER:

“Police and Security Records—VA” (103VA07B).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

VA Police personnel maintains electronic and paper records at VA Central Office and field facilities. Address locations for VA facilities are listed in Appendix 1 of the biennial publication of the VA Privacy Act Issuances.

SYSTEM MANAGER(S):

The Office of Security and Law Enforcement, Director, Police Services is the system owner and provides the business oversight for this SORN and can be contacted at *osle@va.gov*.

The system manager is the Senior Security Officer, Veterans’ Health Administration, Department of Veterans Health Administration, and can be contacted at *vacovhasso@va.gov*.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

38 U.S.C. 501; 38 U.S.C. 901–905.

PURPOSE(S) OF THE SYSTEM:

The records and information contained in this system of records are necessary for the effective administration and management of the Department’s nationwide Security and Law Enforcement Program. The collection and use of accurate, up-to-date data is necessary for the purpose of enforcing the law and protecting persons and property on VA property. Examples: ID cards are used to visibly identify employees, contractors, students, and other designated individuals from the general public. ID cards also serve as a means of access control to a facility. Motor vehicle registration records serve to accurately identify the owner of a vehicle and the suitability of its presence on VA grounds. These records are also used for a VA facility’s ride sharing program. Evidence or confiscated property records are used to accurately track and record the chain of custody maintained by the VA police.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Veterans, VA Police officers, U.S. Government employees, retirees, contractors, subcontractors, volunteers,

and other individuals, including private citizens, who:

1. Have been a complainant, a witness, a victim, or a subject of an investigation of a violation or of an alleged violation of a law on VA property;
2. Have been a witness or a victim when there has been a VA police response to a report of a missing patient;
3. Have been witness to, or involved in, a traffic, motor vehicle or motorized mode of transportation accident on VA property;
4. Have been a witness, victim, or subject when there has been a VA police response to provide assistance to VA employees;
5. Have registered a motor vehicle with VA police;
6. Have had property confiscated by VA police or whose property has been given to VA police for safekeeping; or
7. For whom a VA identification card has been prepared.

CATEGORIES OF RECORDS IN THE SYSTEM:

Police and law enforcement records, containing specific identification of persons, can be found in electronic, audio recordings, digital video recordings and/or security surveillance television (SSTV) recordings and/or paper medium and include:

1. Master Name Index contains demographic information (*i.e.*, name, address, date of birth, sex) and descriptive information such as height, weight, hair color, eye color, and identifying marks (*i.e.*, scars and tattoos).
2. Quick Name Check allows for the immediate retrieval of information based on a name from files contained within the law enforcement records subject to this system of records notice.
3. VA Police Uniform Offense Reports, Investigative Notes, Case Log, and other documentation assembled during an investigation. Incident Reports contain information of all types of offenses and incidents, criminal and non-criminal, that occur at a facility and to which VA Police respond (*e.g.*, criminal investigations, investigative stops, patient and staff assistance calls, missing patient searches, and traffic or motor vehicle accidents).
4. All violation information of U.S. District Court Violation Notices and Courtesy Warnings issued by VA Police.
5. On-station vehicle registration records used for identifying vehicle owners at a facility.
6. Daily Operations Journal records include names and other personal identifying information of persons with whom VA police have had official, duty-related contact.

7. Photographs of any scenes pertinent to an incident or investigation;
8. Motor vehicle registrations, driver’s license, and insurance;
9. Identification cards with photographic images for veterans, U.S. Government employees, retirees, volunteers, contractors, subcontractors, or private citizens;
10. Records of evidence, confiscated property, or property being held for safekeeping.
11. Witness statements and statements of individuals.
12. Records pertaining to individuals, with outstanding warrants, summons, court commitments, or other types of legal processes, and
13. VA Police Training Records.

RECORD SOURCE CATEGORIES:

Information is obtained from Veterans, VA police officers, U.S. Government employees, retirees, volunteers, contractors, subcontractors, other law enforcement agencies, private citizens and other VA information systems.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

1. *Congress:* To a Member of Congress or staff acting upon the Member’s behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

2. *Data Breach Response and Remediation, for VA:* To appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the system of records, (2) VA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, VA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with VA’s efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

3. *Data Breach Response and Remediation, for Another Federal Agency:* To another Federal agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the

Federal Government, or national security, resulting from a suspected or confirmed breach.

4. *Law Enforcement*: To a Federal, State, local, territorial, Tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility of investigating or prosecuting a violation or potential violation of law, whether civil, criminal, or regulatory in nature, or charged with enforcing or implementing such law, provided that the disclosure is limited to information that, either alone or in conjunction with other information, indicates such a violation or potential violation. The disclosure of the names and addresses of veterans and their dependents from VA records under this routine use must also comply with the provisions of 38 U.S.C. 5701.

5. *DoJ, Litigation, Administrative Proceeding*: To the Department of Justice (DoJ), or in a proceeding before a court, adjudicative body, or other administrative body before which VA is authorized to appear, when:

(a) VA or any component thereof;

(b) Any VA employee in his or her official capacity;

(c) Any VA employee in his or her individual capacity where DoJ has agreed to represent the employee; or

(d) The United States, where VA determines that litigation is likely to affect the agency or any of its components, is a party to such proceedings or has an interest in such proceedings, and VA determines that use of such records is relevant and necessary to the proceedings.

6. *Contractors*: To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for VA, when reasonably necessary to accomplish an agency function related to the records.

7. *EEOC*: To the Equal Employment Opportunity Commission (EEOC) in connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or other functions of the Commission as authorized by law.

8. *FLRA*: To the Federal Labor Relations Authority (FLRA) in connection with the investigation and resolution of allegations of unfair labor practices, the resolution of exceptions to arbitration awards when a question of material fact is raised, matters before the Federal Service Impasses Panel, and the investigation of representation petitions and the conduct or supervision of representation elections.

9. *MSPB*: To the Merit Systems Protection Board (MSPB) in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigation of alleged or possible prohibited personnel practices, and such other functions promulgated in 5 U.S.C. 1205 and 1206, or as authorized by law.

10. *NARA*: To the National Archives and Records Administration (NARA) in records management inspections conducted under 44 U.S.C. 2904 and 2906, or other functions authorized by laws and policies governing NARA operations and VA records management responsibilities.

11. *Federal Agencies, for Research*: To a Federal agency for the purpose of conducting research and data analysis to perform a statutory purpose of that Federal agency upon the written request of that agency.

12. *Researchers, for Research*: To epidemiological and other research facilities approved for research purposes determined to be scientifically sound and proper by the Veterans Health Administration Office of Research and Development (ORD), provided that the names and addresses of veterans and their dependents will not be disclosed unless those names and addresses are first provided to VA by the facilities making the request.

13. *Federal Agencies, for Computer Matches*: To other Federal agencies for the purpose of conducting computer matches to obtain information to determine or verify eligibility of veterans receiving VA benefits or medical care under title 38.

14. *Federal Agencies, Courts, Litigants, for Litigation or Administrative Proceedings*: To another Federal agency, court, or party in litigation before a court or in an administrative proceeding conducted by a Federal agency, when the Government is a party to the judicial or administrative proceeding.

15. *Governmental Agencies, Health Organizations, for Claimants' Benefits*: To Federal, State, and local government agencies and national health organizations as reasonably necessary to assist in the development of programs that will be beneficial to claimants, to protect their rights under law, and assure that they are receiving all benefits to which they are entitled.

16. *Governmental Agencies, for VA Hiring, Security Clearance, Contract, License, Grant*: To a Federal, State, local, or other governmental agency maintaining civil or criminal violation records, or other pertinent information, such as employment history, background investigations, or personal

or educational background, to obtain information relevant to VA's hiring, transfer, or retention of an employee, issuance of a security clearance, letting of a contract, or issuance of a license, grant, or other benefit.

17. *Federal Agencies, for Employment*: To a Federal agency, except the United States Postal Service, or to the District of Columbia government, in response to its request, in connection with that agency's decision on the hiring, transfer, or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit by that agency.

18. *State or Local Agencies, for Employment*: To a State, local, or other governmental agency, upon its official request, as relevant and necessary to that agency's decision on the hiring, transfer, or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit by that agency.

19. *Law Enforcement, for Locating Fugitive*: To any Federal, State, local, territorial, Tribal, or foreign law enforcement agency in order to identify, locate, or report a known fugitive felon, in compliance with 38 U.S.C. 5313B(d).

20. *DOD, for Military Mission*: To the Department of Defense, or its components, provided that the disclosure is limited to information regarding individuals treated under 38 U.S.C. 8111A, for the purpose deemed necessary by appropriate military command authorities to assure proper execution of the military.

21. *Federal Register, for Rulemaking*: To make available for public review comments submitted in response to VA's solicitation of public comments as part of the agency's notice and rulemaking activities under the Administrative Procedure Act (APA), provided that the disclosure is limited to information necessary to comply with the requirements of the APA, if VA determines that release of personally identifiable information, such as an individual's telephone number, is integral to the public's understanding of the comment submitted.

24. *Disclosure to Private Insurance Companies*: Information in this system regarding traffic, motor vehicle or motorized mode of transportation (e.g., scooter, wheelchair) accidents may be disclosed to private insurance companies for use in determining payment of a claim under a policy.

25. *Disclosure to VA-appointed Representative*: Disclosure may be made to the VA-appointed representative of an employee of all notices,

determinations, decisions, or other written communications issued to the employee in connection with an examination ordered by VA under medical evaluation (formerly fitness-for-duty) examination procedures or Department filed disability retirement procedures.

26. Client's Attorneys: To assist attorneys in representing their clients, any information in this system may be disclosed to attorneys representing Veterans, U.S. Government employees, retirees, volunteers, contractors, subcontractors, or private citizens being investigated and prosecuted for violating the law, except where VA has decided release is inappropriate under title 5 United States Code, section 552a(j) and (k).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

VA Police Services maintain electronic and paper records at each VA facility.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by name, partial or full social security number, or other personal identifiers.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records will be maintained and disposed of in accordance with the records disposition authority approved by the Archivist of the United States, Veterans Health Administration Records Control Schedule 10–1, Item 525.25.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access to working areas where information is maintained in VA facilities is controlled and restricted to VA employees and VA contractors on a need-to-know basis. Paper document files are locked in a secure container when files are not being used and when work area is not occupied. VA facilities are protected from outside access after normal duty hours by police or security personnel. Access to information on electronic media is controlled by individually unique passwords and codes. Computer access authorizations, computer applications available and used, information access attempts, frequency and time of use are recorded and monitored.

RECORD ACCESS PROCEDURE:

Individuals seeking information on the existence and content of records in this system pertaining to them should write, call or visit the VA facility where the records are maintained.

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest or amend records in this system pertaining to them should write, call or visit the VA facility where the records are maintained. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record. A majority of records in this system are exempt from record access and amendment provisions of Title 5 U.S.C., Sections 552a(j) and (k). To the extent that records in this system are not subject to exemption, individuals may request access and/or amendment. A determination as to whether an exemption applies shall be made at the time a request for access or contest is received.

NOTIFICATION PROCEDURES:

Generalized notice is provided by the publication of this notice. For specific notice, see Record Access Procedure, above.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

Under title 5 U.S.C., section 552a(j)(2), the head of any agency may exempt any system of records within the agency from certain provisions of the Privacy Act, if the agency or component that maintains the system performs as its principal function any activities pertaining to the enforcement of criminal laws. The function of the Police Service is to provide for the maintenance of law and order and the protection of persons and property on Department property. This system of records has been created, in major part, to support the law enforcement related activities assigned by the Department under the authority of title 38 U.S.C., section 901 to the Police Service. These activities constitute the principal function of this staff.

In addition to principal functions pertaining to the enforcement of criminal laws, the Police Service may receive and investigate complaints or

information from various sources concerning the possible existence of activities constituting noncriminal violations of law, rules, or regulations or substantial and specific danger to the public and safety.

Based upon the foregoing, the Secretary of Veterans Affairs (VA) has exempted this system of records, to the extent that it encompasses information pertaining to criminal law enforcement related activities from the following provisions of the Privacy Act of 1974, as permitted by 5 U.S.C. 552a(j)(2):

- 5 U.S.C. 552a(c)(3) and (4).
- 5 U.S.C. 552a(d)(1) through (4).
- 5 U.S.C. 552a(e)(1), (2) and (3).
- 5 U.S.C. 552a(e)(4)(G), (H) and (I). 5 U.S.C. 552a(e)(5) and (8).
- 5 U.S.C. 552a(f).
- 5 U.S.C. 552a(g).

The Secretary of Veterans Affairs has exempted this system of records, to the extent that it does not encompass information pertaining to criminal law enforcement related activities under 5 U.S.C. 552a(j)(2), from the following provisions of the Privacy Act of 1974, as permitted by 5 U.S.C. 552a(k)(2):

- 5 U.S.C. 552a(c)(3).
- 5 U.S.C. 552a(d)(1) through (4). 5 U.S.C. 552a(e)(1).
- 5 U.S.C. 552a(e)(4)(G), (H) and (I). 5 U.S.C. 552a(f).

Reasons for exemptions: The exemption of information and material in this system of records is necessary in order to accomplish the law enforcement functions of the Police Service, to prevent subjects of investigations from frustrating the investigatory process, to prevent the disclosure of investigative techniques, to fulfill commitments made to protect the confidentiality of sources, to maintain access to sources of information, and to avoid endangering these sources and Police personnel.

HISTORY:

Federal Register at 87 FR 64141, Friday, October 21, 2022; 67 FR 77737 (December 19, 2002); 73 FR 74580 (December 8, 2008).

[FR Doc. 2024–07137 Filed 4–3–24; 8:45 am]

BILLING CODE 8320–01–P



FEDERAL REGISTER

Vol. 89

Thursday,

No. 66

April 4, 2024

Part II

Department of Homeland Security

Cybersecurity and Infrastructure Security Agency

6 CFR Part 226

Cyber Incident Reporting for Critical Infrastructure Act (CIR CIA) Reporting Requirements; Proposed Rule

DEPARTMENT OF HOMELAND SECURITY

Cybersecurity and Infrastructure Security Agency

6 CFR Part 226

[Docket No. CISA–2022–0010]

RIN 1670–AA04

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

AGENCY: Cybersecurity and Infrastructure Security Agency, DHS

ACTION: Proposed rule.

SUMMARY: The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as amended, requires the Cybersecurity and Infrastructure Security Agency (CISA) to promulgate regulations implementing the statute's covered cyber incident and ransom payment reporting requirements for covered entities. CISA seeks comment on the proposed rule to implement CIRCIA's requirements and on several practical and policy issues related to the implementation of these new reporting requirements.

DATES: Comments and related material must be submitted on or before June 3, 2024.

ADDRESSES: You may send comments, identified by docket number CISA–2022–0010, through the Federal eRulemaking Portal available at <http://www.regulations.gov>.

Instructions: All comments received must include the docket number for this rulemaking. All comments received will be posted to <https://www.regulations.gov>, including any personal information provided. If you cannot submit your comment using <https://www.regulations.gov>, contact the person in the **FOR FURTHER INFORMATION CONTACT** section of this proposed rule for alternate instructions. For detailed instructions on sending comments and additional information on the types of comments that are of particular interest to CISA for this proposed rulemaking, see the "Public Participation" heading of the **SUPPLEMENTARY INFORMATION** section of this document.

Docket: For access to the docket and to read background documents mentioned in this proposed rule and comments received, go to <https://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: Todd Klessman, CIRCIA Rulemaking Team Lead, Cybersecurity and Infrastructure Security Agency, circia@cisa.dhs.gov, 202–964–6869.

SUPPLEMENTARY INFORMATION:

Table of Contents

- I. Public Participation
- II. Executive Summary
 - A. Purpose and Summary of the Regulatory Action
 - B. Summary of Costs and Benefits
- III. Background and Purpose
 - A. Legal Authority
 - B. Current Cyber Incident Reporting Landscape
 - C. Purpose of Regulation
 - i. Purposes of the CIRCIA Regulation
 - ii. How the Regulatory Purpose of CIRCIA Influenced the Design of the Proposed CIRCIA Regulation
 - D. Harmonization Efforts
 - E. Information Sharing Required by CIRCIA
 - F. Summary of Stakeholder Comments
 - i. General Comments
 - ii. Comments on the Definition of Covered Entity
 - iii. Comments on the Definition of Covered Cyber Incident and Substantial Cyber Incident
 - iv. Comments on Other Definitions
 - v. Comments on Criteria for Determining Whether the Domain Name System Exception Applies
 - vi. Comments on Manner and Form of Reporting, Content of Reports, and Reporting Procedures
 - vii. Comments on the Deadlines for Submission of CIRCIA Reports
 - viii. Comments on Third-Party Submitters
 - ix. Comments on Data and Records Preservation Requirements
 - x. Comments on Other Existing Cyber Incident Reporting Requirements and the Substantially Similar Reporting Exception
 - xi. Comments on Noncompliance and Enforcement
 - xii. Comments on Treatment and Restrictions on Use of CIRCIA Reports
- IV. Discussion of Proposed Rule
 - A. Definitions
 - i. Covered Entity
 - ii. Cyber Incident, Covered Cyber Incident, and Substantial Cyber Incident
 - iii. CIRCIA Reports
 - iv. Other Definitions
 - v. Request for Comments on Proposed Definitions
 - B. Applicability
 - i. Interpreting the CIRCIA Statutory Definition of Covered Entity
 - ii. Determining if an Entity Is in a Critical Infrastructure Sector
 - iii. Clear Description of the Types of Entities That Constitute Covered Entities Based on Statutory Factors
 - iv. Explanation of Specific Proposed Applicability Criteria
 - v. Other Approaches Considered To Describe Covered Entity
 - vi. Request for Comments on Applicability Section
 - C. Required Reporting on Covered Cyber Incidents and Ransom Payments
 - i. Overview of Reporting Requirements
 - ii. Reporting of Single Incidents Impacting Multiple Covered Entities
 - D. Exceptions to Required Reporting on Covered Cyber Incidents and Ransom Payments

- i. Substantially Similar Reporting Exception
- ii. Domain Name System (DNS) Exception
- iii. Exception for Federal Agencies Subject to Federal Information Security Modernization Act Reporting Requirements
- E. Manner, Form, and Content of Reports
 - i. Manner of Reporting
 - ii. Form for Reporting
 - iii. Content of Reports
 - iv. Timing of Submission of CIRCIA Reports
 - v. Report Submission Procedures
 - vi. Request for Comments on Proposed Manner, Form, and Content of Reports
- F. Data and Records Preservation Requirements
 - i. Types of Data That Must Be Preserved
 - ii. Required Preservation Period
 - iii. Data Preservation Procedural Requirements
 - iv. Request for Comments on Proposed Data Preservation Requirements
- G. Enforcement
 - i. Overview
 - ii. Request for Information
 - iii. Subpoena
 - iv. Service of an RFI, Subpoena, or Notice of Withdrawal
 - v. Enforcement of Subpoenas
 - vi. Acquisition, Suspension, and Debarment Enforcement Procedures
 - vii. Penalty for False Statements and Representations
 - viii. Request for Comments on Proposed Enforcement
- H. Protections
 - i. Treatment of Information and Restrictions on Use
 - ii. Protection of Privacy and Civil Liberties
 - iii. Digital Security
 - iv. Request for Comments on Proposed Protections
- I. Severability
- V. Statutory and Regulatory Analyses
 - A. Regulatory Planning and Review
 - i. Number of Reports
 - ii. Industry Cost
 - iii. Government Cost
 - iv. Combined Costs
 - v. Benefits
 - vi. Accounting Statement
 - vii. Alternatives
 - B. Small Entities
 - C. Assistance for Small Entities
 - D. Collection of Information
 - E. Federalism
 - F. Unfunded Mandates Reform Act
 - G. Taking of Private Property
 - H. Civil Justice Reform
 - I. Protection of Children
 - J. Indian Tribal Governments
 - K. Energy Effects
 - L. Technical Standards
 - M. National Environmental Policy Act
- VI. Proposed Regulation

List of Tables

- Table 1: Affected Population, by Criteria
- Table 2: Number of CIRCIA Reports, Primary Estimate
- Table 3: Number of CIRCIA Reports
- Table 4: Familiarization Cost by Entity Type, Primary Estimate
- Table 5: Total Familiarization Costs (\$ Millions, Undiscounted)

Table 6: Cost of CIRCIA Reporting
 Table 7: Data and Record Preservation Costs
 Table 8: Industry Cost Range, (\$ Millions, Undiscounted)
 Table 9: Total Industry Cost, Primary Estimate (\$ Millions)
 Table 10: Cost by Covered Entity Criteria, (\$ Millions, Undiscounted)
 Table 11: Government Cost (\$ Millions)
 Table 12: Combined Industry and Government Cost, Primary Estimate (\$ Millions)
 Table 13: Combined Industry and Government Cost Range, (\$ Millions)
 Table 14: Summary of Cyber Event Losses and Counts, IRIS 2022
 Table 15: OMB A-4 Accounting Statement (\$ Millions, 2022 Dollars)
 Table 16: Alternative 1 Industry Cost, Primary Estimate (\$ Millions)
 Table 17: Alternative 1 Combined Industry and Government Cost, Primary Estimate, (\$ Millions)
 Table 18: Alternative 2 Industry Cost, Primary Estimate (\$ Millions)
 Table 19: Alternative 2 Combined Industry and Government Cost, Primary Estimate (\$ Millions)
 Table 20: Alternative 3 Industry Cost, Primary Estimate (\$ Millions)
 Table 21: Alternative 3 Combined Industry and Government Cost, Primary Estimate (\$ Millions)
 Table 22: Affected Population by Critical Infrastructure Sector
 Table 23: Alternative 4 Industry Cost, Primary Estimate (\$ Millions)
 Table 24: Alternative 4 Combined Industry and Government Costs, Primary Estimate (\$ Millions)
 Table 25: Alternatives Summary, Combined Industry and Government Cost, Primary Estimate (\$ Millions)

Abbreviations and Acronyms Frequently Used in This Document

ARIN American Registry for Internet Numbers
 ATO Authority to Operate
 BES Bulk Electric System
 CFATS Chemical Facility Anti-Terrorism Standards
 CFTC Commodity Futures Trading Commission
 CHS U.S. House Committee on Homeland Security
 CIA Confidentiality, Integrity, and Availability
 CIP Critical Infrastructure Protection
 CIRC Cyber Incident Reporting Council
 CIRCIA Cyber Incident Reporting for Critical Infrastructure Act of 2022, as amended
 CISA Cybersecurity and Infrastructure Security Agency
 CSP Cloud Service Provider
 DFARS Defense Federal Acquisition Regulation Supplement
 DHS Department of Homeland Security
 DNS Domain Name System
 DOD Department of Defense
 DOE Department of Energy
 DOJ Department of Justice
 EPA Environmental Protection Agency
 ESA Educational Service Agency
 FBI Federal Bureau of Investigation

FCC Federal Communications Commission
 FDA Food and Drug Administration
 FDIC Federal Deposit Insurance Corporation
 FedRAMP Federal Risk and Authorization Management Program
 FERC Federal Energy Regulatory Commission
 FHFA Federal Housing Finance Agency
 FICU Federally Insured Credit Union
 FISMA Federal Information Security Modernization Act of 2014
 FOIA Freedom of Information Act
 FRB Federal Reserve Board
 GAO Government Accountability Office
 GCC Government Coordinating Council
 GSA General Services Administration
 gTLD Generic Top-Level Domain
 HHS Department of Health and Human Services
 HIPAA Health Insurance Portability and Accountability Act of 1996
 HITECH Health Information Technology for Economic and Clinical Health
 HSGAC U.S. Senate Committee on Homeland Security and Governmental Affairs
 IANA Internet Assigned Numbers Authority
 ICANN Internet Corporation for Assigned Names and Numbers
 ICT Information and Communications Technology
 IHE Institute of Higher Education
 IP Internet Protocol
 ISAC Information Sharing and Analysis Center
 IT Information Technology
 K-12 Kindergarten through 12th Grade
 LEA Local Educational Agency
 MTSA Maritime Transportation Security Act
 NAICS North American Industry Classification System
 NCF National Critical Function
 NCUA National Credit Union Administration
 NERC North American Electric Reliability Corporation
 NIPP National Infrastructure Protection Plan
 NIST National Institute of Standards and Technology
 NORS Network Outage Reporting System
 NPRM Notice of Proposed Rulemaking
 NRC Nuclear Regulatory Commission
 NSA National Security Agency
 OCC Office of the Comptroller of the Currency
 OEM Original Equipment Manufacturer
 OMB Office of Management and Budget
 OT Operational Technology
 OTRB Over-the-Road Bus
 POTW Publicly Owned Treatment Works
 PPD Presidential Policy Directive
 PRA Paperwork Reduction Act
 PTPR Public Transportation and Passenger Railroads
 RFI Request for Information
 RIR Regional Internet Registry
 RTR Research and Test Reactor
 RSO Root Server Operator
 SBA Small Business Administration
 SCC Sector Coordinating Council
 SEA State Educational Agency
 SEC Securities and Exchange Commission
 SLTT State, Local, Tribal, or Territorial

SRMA Sector Risk Management Agency
 SSP Sector-Specific Plan
 TLD Top-Level Domain
 TSA Transportation Security Administration
 TTP Tactics, Techniques, and Procedures
 USCG United States Coast Guard
 USDA United States Department of Agriculture
 VoIP Voice over Internet Protocol

I. Public Participation

The Cybersecurity and Infrastructure Security Agency (CISA) views public participation as essential to effective rulemaking and invites interested persons to participate by submitting data, comments, and other information on the content and assumptions made in this proposed rule. Your comments can help shape the outcome of this rulemaking. CISA is particularly interested in comments on the following:

a. *Proposed Definitions.* The proposed definition of covered cyber incident and the other definitions CISA is proposing to include in the regulation (see proposed § 226.1 and Section IV.A in this document);

b. *Applicability.* The proposed description of covered entity, the scope of entities to whom this regulation applies (see proposed § 226.2 and Section IV.B in this document);

c. *Examples of Reportable Covered Cyber Incidents.* The examples of substantial cyber incidents included in this Notice of Proposed Rulemaking (NPRM) (see Section IV.A.ii.3.e in this document);

d. *CIRCIA Reporting Requirements and Procedures.* The proposed reporting requirements and procedures for CIRCIA Reports, specifically the manner, form, and content of CIRCIA Reports (see proposed §§ 226.6 through 226.12 and Section IV.E.i-iii in this document), including CISA's proposal to use a single, dynamic, web-based form as the primary means of submission for all CIRCIA Reports (see Section IV.E.i.2 in this document);

e. *Proposed CIRCIA Report Submission Deadlines.* The proposed deadlines for submitting CIRCIA Reports and CISA's proposed interpretations of these submission deadline requirements (see proposed § 226.5 and Section IV.E.iv in this document);

f. *Data and Records Preservation Requirements.* The proposed data and records preservation requirements and preservation period (see proposed § 226.13 and Section IV.F in this document);

g. *Enforcement Procedures.* The proposed enforcement procedures, including the procedures related to

issuance of a Request for Information (RFI) or subpoena and the proposed subpoena withdrawal and appeals process (see proposed §§ 226.14 through 226.17 and Section IV.G in this document);

h. *Treatment of Information and Restrictions on Use.* The proposed rules governing the protections and restrictions on the use of CIRCIA Reports, information included in such reports, and responses to RFIs (see proposed § 226.18 and Section IV.H.i in this document); and

i. *Procedures for Protecting Privacy and Civil Liberties.* The proposed procedures governing the protection of personal information contained in CIRCIA Reports and responses to RFIs (see proposed § 226.19 and Section IV.H.ii in this document), which are further described in the draft Privacy and Civil Liberties Guidance for CIRCIA (this draft document is available in the docket for this proposed regulatory action (CISA–2022–0010)).

CISA is including in the docket a draft privacy and civil liberties guidance document that would apply to CISA's retention, use, and dissemination of personal information contained in a CIRCIA Report and guide other Federal departments and agencies with which CISA will share CIRCIA Reports. CISA encourages interested readers to review this draft guidance and to submit comments on it. Commenters should clearly identify which specific comment(s) concern the draft guidance document.

CISA will accept comments no later than the date provided in the **DATES** section of this document. Interested parties may submit data, comments, and other information using any of the methods described in the **ADDRESSES** section of this document. To ensure appropriate consideration of your comment, indicate the specific section of this proposed rule and, if applicable, the specific comment request number associated with the topic to which each comment applies; explain a reason for any suggestion or recommendation; and include data, information, or authority that supports the recommended course of action. Comments submitted in a manner other than those described above, including emails or letters sent to Department of Homeland Security (DHS) or CISA officials, will not be considered comments on the proposed rule and may not receive a response from CISA.

Instructions to Submit Comments. If you submit a comment, you must submit it to the docket associated with CISA Docket Number CISA–2022–0010. All submissions may be posted, without

change, to the Federal eRulemaking Portal at www.regulations.gov and will include any personal information that you provide. You may choose to submit your comment anonymously.

Additionally, you may upload or include attachments with your comments. Do not upload any material in your comments that you consider confidential or inappropriate for public disclosure. Do not submit comments that include trade secrets, confidential commercial or financial information, Protected Critical Infrastructure Information, Sensitive Security Information, or any other protected information to the public regulatory docket. Please submit comments containing protected information separately from other comments by contacting the individual listed in the **FOR FURTHER INFORMATION CONTACT** section of this document for instructions on how to submit comments that include protected information. CISA will not place comments containing protected information in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. CISA will hold such comments in a separate file to which the public does not have access and place a note in the public docket documenting receipt. If CISA receives a request for a copy of any comments submitted containing protected information, CISA will process such a request consistent with the Freedom of Information Act (FOIA), 5 U.S.C. 552, and the Department's FOIA regulation found in part 5 of title 6 of the Code of Federal Regulations (CFR).

To submit a comment, go to www.regulations.gov, type CISA–2022–0010 in the search box and click "Search." Next, look for this **Federal Register** notice of proposed rulemaking in the Search Results column, and click on it. Then click on the Comment option. If you cannot submit your comment by using <https://www.regulations.gov>, call or email the point of contact in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions.

Viewing material in docket. For access to the docket and to view documents mentioned in this NPRM as being available in the docket, go to <https://www.regulations.gov>, search for the docket number provided in the previous paragraph, and then select "Supporting & Related Material" in the Document Type column. Public comments will also be placed in the docket and can be viewed by following instructions on the Frequently Asked Questions web page <https://www.regulations.gov/faq>. The

Frequently Asked Questions page also explains how to subscribe for email alerts that will notify you when comments are posted or if another **Federal Register** document is published. CISA will review all comments received. CISA may choose to withhold information provided in comments from public viewing or to not post comments that CISA determines are off-topic or inappropriate.

Public meeting. CISA does not plan to hold additional public meetings at this time, but may consider doing so if CISA determines from public comments that a meeting would be helpful. If CISA decides to hold a public meeting, a notice announcing the date, time, and location for the meeting will be issued in a separate **Federal Register** notice.

II. Executive Summary

A. Purpose and Summary of the Regulatory Action

On March 15, 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law. See 6 U.S.C. 681–681g; Public Law 117–103, as amended by Public Law 117–263 (Dec. 23, 2022). CIRCIA requires covered entities to report to CISA within certain prescribed timeframes any covered cyber incidents, ransom payments made in response to a ransomware attack, and any substantial new or different information discovered related to a previously submitted report. 6 U.S.C. 681b(a)(1)–(3). CIRCIA further requires the Director of CISA to implement these new reporting requirements through rulemaking, by issuing an NPRM no later than March 15, 2024, and a final rule within 18 months of publication of the NPRM. 6 U.S.C. 681b(b). CISA is issuing this NPRM to solicit public comment on proposed regulations that would codify these reporting requirements.

This NPRM is divided into six sections. Section I—Public Participation describes the process for members of the public to submit comments on the proposed regulations and lists specific topics on which CISA is particularly interested in receiving public comment. Section II—Executive Summary contains a summary of the proposed regulatory action and the anticipated costs and benefits of the proposed regulations. Section III—Background and Purpose contains a summary of the legal authority for this proposed regulatory action; an overview of the current regulatory cyber incident reporting landscape; a description of the purpose of the proposed regulations; a discussion of efforts CISA has taken to

harmonize these proposed regulations with other Federal cyber incident reporting regulations; a discussion of information sharing activities related to the proposed regulations; and a summary of the comments CISA received in response to an RFI issued by CISA on approaches to the proposed regulations and during listening sessions hosted by CISA on the same topic. Section IV—Discussion of Proposed Rule includes a detailed discussion of the proposed rule, the justification for CISA's specific proposals, and the alternatives considered by CISA. Section V—Statutory and Regulatory Analyses contains the analyses that CISA is required by statute or Executive Order to perform as part of the rulemaking process prior to issuance of the final rule, such as the Initial Regulatory Flexibility Analysis and Unfunded Mandates Reform Act analysis. Section VI contains the proposed regulatory text.

The proposed rule is comprised of 20 sections, §§ 226.1 through 226.20, beginning with a section containing definitions for a number of key terms used throughout the proposed regulation. Among other definitions, § 226.1 includes proposed definitions for the terms used to describe and ultimately scope what types of incidents must be reported to CISA (*i.e.*, cyber incident, covered cyber incident, ransom payment, and substantial cyber incident) and the term used to describe the different types of reports that must be submitted (*i.e.*, CIRCIA Reports).

The next section of the proposed rule, § 226.2, describes the applicability of the proposed rule to certain entities in a critical infrastructure sector, *i.e.*, those entities that are considered covered entities and to whom the operative provisions of the rule would apply.

The next section of the proposed rule, § 226.3, describes the circumstances under which a covered entity must submit a CIRCIA Report to CISA. This includes when a covered entity experiences a covered cyber incident, makes a ransom payment, has another entity make a ransom payment on its behalf, or acquires substantial new or different information after submitting a previous CIRCIA Report. See § 226.3; Section IV.C in this document. CISA is proposing three exceptions to these reporting requirements for covered entities, which are in § 226.4 of the proposed regulation and described in Section IV.D in this document. These exceptions include when a covered entity reports substantially similar information in a substantially similar timeframe to another Federal agency

pursuant to an existing law, regulation, or contract when a CIRCIA Agreement is in place between CISA and the other Federal agency; when an incident impacts certain covered entities related to the Domain Name System (DNS); and when Federal agencies are required by the Federal Information Security Modernization Act of 2014 (FISMA) to report incidents to CISA. See § 226.4 of the proposed regulation and Section IV.D of this document.

Section 226.5 of the proposed regulation contains the submission deadlines for the four different types of CIRCIA Reports (*i.e.*, Covered Cyber Incident Reports; Ransom Payment Reports; Joint Covered Cyber Incident and Ransom Payment Reports; Supplemental Reports). These deadlines, including how to calculate them, are discussed further in Section IV.E.iv in this document. Section 226.6 of the proposed regulation sets forth the proposed manner and form of reporting, which CISA proposes to be through a web-based CIRCIA Incident Reporting Form available on CISA's website or in any other manner and form of reporting approved by the Director. Additional details on the proposed manner and form of reporting and related submission procedures are contained in Sections IV.E.i, ii and v in this document. The information CISA proposes that covered entities must include in each of the four types of CIRCIA Reports is enumerated in §§ 226.7 through 226.11 and expanded upon in Section IV.E.iii in this document.

A covered entity may use a third party to submit a CIRCIA Report to CISA on the covered entity's behalf to satisfy the covered entity's reporting obligations. See 6 U.S.C. 681b(d). The proposed procedures and requirements for using a third party to submit a CIRCIA Report on behalf of the covered entity are contained in § 226.12 of the proposed regulations and discussed in detail in Section IV.E.v.3 in this document. The proposed regulation also affirms the statutorily mandated obligation for a third party to advise the covered entity of its ransom payment reporting obligations under CIRCIA when the third party knowingly makes a ransom payment on behalf of a covered entity. See 6 U.S.C. 681b(d)(4), § 226.12(d) of the proposed regulations, and Section IV.E.v.3.e of the NPRM.

Section 226.13 of the proposed regulation sets forth the proposed data and records preservation requirements. It includes a recitation of the types of data and records that a covered entity must preserve; the required preservation period; the format or form in which the

data and records must be preserved; and the storage, protection, and allowable uses of the preserved data and records. See § 226.13 and Section IV.F in this document.

CIRCIA authorizes CISA to use various mechanisms to obtain information from a covered entity about a covered cyber incident or ransom payment that was not reported in accordance with CISA's proposed regulatory reporting requirements. 6 U.S.C. 681d. These mechanisms include the issuance of an RFI; the issuance of a subpoena; a referral to the Attorney General to bring a civil action in District Court to enforce a subpoena; and acquisition, suspension, and debarment enforcement procedures. The proposed procedures for each of these enforcement mechanisms are contained in §§ 226.14 through 226.17 of the proposed regulation and discussed in Section IV.G.i–vi in this document.

CIRCIA provides a variety of requirements related to the treatment and restrictions on the use of CIRCIA Reports, information contained in such reports, as well as information submitted in response to an RFI. See 6 U.S.C. 681e(b), 681e(a)(1), (5). CIRCIA also provides liability protection for the submission of a CIRCIA Report in compliance with the reporting requirements established in the CIRCIA regulation. 6 U.S.C. 681e(c). To ensure that such requirements related to the treatment and restrictions on the use of CIRCIA Reports are applied consistently, CISA proposes to include them in § 226.18, as discussed in Section IV.H.i in this document. CISA additionally proposes steps to minimize the collection of unnecessary personal information in CIRCIA Reports and additional procedures for protecting privacy and civil liberties related to the submission of CIRCIA Reports and responses to RFIs. These proposed procedures for protecting privacy and civil liberties are contained in § 226.19 of the proposed regulation and discussed further in Section IV.H.ii in this document as well as in the guidance document posted to the docket for this proposed rule.

The final section of the proposed regulation, § 226.20, proposes two distinct procedural provisions. The first proposed provision provides that any person who knowingly and willfully makes a materially false or fraudulent statement or representation in connection with, or within, a CIRCIA Report, RFI response, or reply to an administrative subpoena is subject to penalties under 18 U.S.C. 1001. § 226.20(a). The second proposed provision is a severability clause, which

states CISA intends the various provisions of this part to be severable from each other to the extent practicable, such that if a court of competent jurisdiction were to vacate or enjoin any one provision, the other provisions remain in effect unless they are dependent upon the vacated or enjoined provision. § 226.20(b). These are discussed in Sections IV.G.vii and IV.I in this document, respectively.

B. Summary of Costs and Benefits

CISA estimates the cost of this proposed rule would be \$2.6 billion over the period of analysis¹ (undiscounted). CISA estimates that there will be 316,244 entities potentially affected by the proposed rule (*i.e.*, covered entities) who collectively will submit an estimated total of 210,525 CIRCIA Reports over the period of analysis, resulting in \$1.4 billion (undiscounted) in cost to industry and \$1.2 billion (undiscounted) in cost to the Federal Government. The cost over the period of analysis discounted at 2% would be \$2.4 billion (\$1.3 billion for industry, \$1.1 billion for government), with an annualized cost of \$244.6 million, as presented in the Preliminary Regulatory Impact Analysis (RIA) included in the docket. The main industry cost drivers of this proposed rule are the initial costs associated with becoming familiar with the proposed rule, followed by the recurring data and records preservation requirements, and then reporting requirements. Other industry costs include those associated with help desk calls and enforcement actions. Government costs include costs CISA anticipates incurring associated with the creation, implementation, and operation of the government infrastructure needed to run the CIRCIA program. This includes both personnel and technology costs necessary to support the receipt, analysis, and sharing of information from CIRCIA Reports submitted to CISA.

The Preliminary RIA also discusses the qualitative benefits of the proposed rule. From a qualitative benefits perspective, the proposed reporting requirements, analytical activities, and information sharing will lead to Federal and non-Federal stakeholders having the ability to adopt an enhanced overall level of cybersecurity and resiliency,

resulting in direct, tangible benefits to the nation. For example:

- By supporting CISA's ability to share information that will enable non-Federal and Federal partners to detect and counter sophisticated cyber campaigns earlier with the potential for significant avoided or minimized negative impacts to critical infrastructure or national security, CIRCIA's mandatory reporting requirements reduce the risks associated with those campaigns.

- By facilitating the identification and sharing of information on exploited vulnerabilities and measures that can be taken to address those vulnerabilities, incident reporting enables entities with unremediated and unmitigated vulnerabilities on their systems to take steps to remedy or mitigate those vulnerabilities before they also fall victim to cyberattack.

- By supporting sharing of information about common threat actor tactics, techniques, and procedures with the IT community, cyber incident reporting will enable software developers and vendors to develop more secure products or send out updates to add security to existing products, better protecting end users.

- By enabling rapid identification of ongoing incidents and increased understanding of successful mitigation measures, incident reporting increases the ability of impacted entities and the Federal government to respond to ongoing campaigns faster and mitigate or minimize the consequences that could result from them.

- Law enforcement entities can use the information submitted in reports to investigate, identify, capture, and prosecute perpetrators of cybercrime, getting malicious cyber actors off the street and deterring future actors.

- By contributing to a more accurate and comprehensive understanding of the cyber threat environment, incident reporting allows for CISA's Federal and non-Federal stakeholders to more efficiently and effectively allocate resources to prevent, deter, defend against, respond to, and mitigate significant cyber incidents.

These benefits, which stem from CISA receiving cyber incident and ransom payment reporting for aggregation, analysis, and information sharing, directly contribute to a reduction in economic, health, safety, and security consequences associated with cyber incidents by reducing the number of cyber incidents successfully perpetrated and mitigating the consequences of those cyber incidents that are successful by catching them earlier. It is worth noting that these benefits are not limited

to covered entities required to report under CIRCIA, but also inure to entities not subject to CIRCIA's reporting requirements as they too will receive the downstream benefits of enhanced information sharing, more secure technology products, and an ability to better defend their networks based on sector-specific and cross-sector understandings of the threat landscape.

CISA also anticipates qualitative benefits stemming from the data and record preservation requirements of this proposed rule. The preservation of data and records in the aftermath of a covered cyber incident serves a number of critical purposes, such as supporting the ability of analysts and investigators to understand how a cyber incident was perpetrated and by whom.

III. Background and Purpose

A. Legal Authority

On March 15, 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was signed into law. See 6 U.S.C. 681–681g; Public Law 117–103, as amended by Public Law 117–263 (Dec. 23, 2022). CIRCIA requires covered entities to report to CISA covered cyber incidents within 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred and ransom payments made in response to a ransomware attack within 24 hours after the ransom payment has been made. 6 U.S.C. 681b(a). Among other benefits, this new authority will enhance CISA's ability to identify trends and track cyber threat activity across the cyber threat landscape beyond the Federal agencies that are already required to report information on certain cyber incidents to CISA pursuant to the FISMA, 44 U.S.C. 3554(b)(7)(C)(ii) and 6 U.S.C. 652(c)(3). CIRCIA requires the Director of CISA to implement these new reporting requirements through rulemaking, by issuing a Notice of Proposed Rulemaking no later than March 15, 2024, and a final rule within 18 months of the NPRM's publication. 6 U.S.C. 681b(b).

CIRCIA also authorizes CISA to request information and engage in administrative enforcement actions to compel a covered entity to disclose information if it has failed to comply with its reporting obligations. 6 U.S.C. 681d. CIRCIA establishes information treatment requirements and restrictions on use, including certain protections against liability and exemptions from public disclosure, for required reports and information submitted to CISA. 6 U.S.C. 681e, 681d(b)(2), 681c(c). CIRCIA also provides for Federal interagency

¹ CISA used an 11-year period of analysis spanning from 2023–2033 to reflect that CISA began incurring costs related to CIRCIA implementation in 2023, one year prior to the publication of the NPRM. See the Executive Summary section of the *CIRCIA Regulation Proposed Rulemaking Preliminary Regulatory Impact Analysis and Initial Regulatory Flexibility Analysis* for additional detail on the period of analysis.

coordination and sharing of information on cyber incidents, including ransomware attacks, reported to Federal departments and agencies, and covered cyber incidents and ransom payments reported to CISA. 6 U.S.C. 681a(a)(10), (b), 681g.

Although CIRCIA requires CISA to implement new reporting requirements through regulation, CISA's rulemaking authority under CIRCIA does not supersede, abrogate, modify, or otherwise limit any authority to regulate or act with respect to the cybersecurity of an entity vested in any United States Government officer or agency. 6 U.S.C. 681b(h). Therefore, covered entities that are obligated to report covered cyber incidents or ransom payments pursuant to another Federal regulatory requirement, directive, or similar mandate will remain obligated to do so even if the reporting requirements differ from those established by CIRCIA. Where CIRCIA imposes regulatory requirements that may overlap or duplicate other Federal regulatory requirements, CISA is committed to working with other Federal partners to explore options to minimize unnecessary duplication between CIRCIA's reporting requirements and other Federal cyber incident reporting requirements and welcomes public comment regarding options to minimize unnecessary duplication or identification of specific Federal cyber incident reporting requirements where such duplication is likely to occur. Additionally, CIRCIA does not permit or require a provider of a remote computing service or electronic communication service to the public to disclose information not otherwise permitted or required to be disclosed under 18 U.S.C. 2701–2713 (commonly known as the “Stored Communications Act”). 6 U.S.C. 681e(e).

CIRCIA also provides that entities may voluntarily report cyber incidents or ransom payments to CISA that are not required to be reported under the CIRCIA regulations, and applies the same information treatment requirements on use (including liability protections) and restrictions on use to such voluntarily submitted reports. 6 U.S.C. 681c(a), (c); 681e. CISA is not, however, proposing to address entirely voluntary reporting (e.g., how such reports may be submitted) in this rulemaking.

B. Current Cyber Incident Reporting Landscape

The cyber incident reporting landscape currently consists of dozens of Federal and state, local, tribal, or territorial (SLTT) cyber incident

reporting requirements that may apply to entities operating within the United States, depending on where an entity or its customers are located and the type of business in which the entity is engaged. At the Federal level alone, more than three dozen different cyber incident reporting requirements currently are in effect, with a number of additional proposed regulatory reporting requirements in various stages of development. At the SLTT level, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, and all 50 states have laws that require reporting and/or public disclosure of at least some cyber incidents that result in data breaches.

Despite these myriad Federal and SLTT reporting requirements, prior to the enactment of CIRCIA, there was no Federal statute or regulation supporting a comprehensive and coordinated approach to understanding cyber incidents across critical infrastructure sectors. Nor was there a Federal department or agency charged with coordinating cross-sector sharing of information related to cyber incidents with Federal and non-Federal stakeholders. Indeed, during the lead up to the passage of CIRCIA, Congress stated “[t]oday no one U.S. Government agency has visibility into all cyberattacks occurring against U.S. critical infrastructure on a daily basis. This bill would change that—enabling a coordinated, informed U.S. response to the foreign governments and criminal organizations conducting these attacks against the U.S.”² The enactment of CIRCIA authorized CISA to fill these key gaps in the current cyber incident reporting landscape.

There are a number of different reasons why a government entity may establish cyber incident reporting requirements. A recent DHS report to Congress based on the work of the Cyber Incident Reporting Council (CIRC)³ titled *Harmonization of Cyber Incident Reporting to the Federal Government* suggests that these reasons generally can be organized into two primary categories.⁴ The first category consists of

² U.S. Senate Committee on Homeland Security and Governmental Affairs (HSGAC), *Cyber Incident Reporting for Critical Infrastructure Act* at 1 (Dec. 17, 2021), available at <https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Overview%20of%20Cyber%20Incident%20Reporting%20Legislation.pdf> (hereinafter, “HSGAC Fact Sheet”).

³ CIRCIA established an intergovernmental Cyber Incident Reporting Council. Chaired by the Secretary of Homeland Security, the CIRC is responsible for coordinating, deconflicting, and harmonizing Federal incident reporting requirements, including those issued through regulations. 6 U.S.C. 681f.

⁴ Department of Homeland Security, *Harmonization of Cyber Incident Reporting to the*

regulations primarily focused on national security, economic security, public health and safety, and/or the resiliency of National Critical Functions (NCFs). A majority of Federal reporting regimes appear to be solely or primarily animated by these concerns. The remaining Federal cyber incident reporting regimes, as well as virtually all SLTT cyber incident reporting regimes, are designed primarily to address privacy, consumer protection, or investor protection considerations. This second category includes all the reporting regimes often referred to as data breach notification laws.

Outside of state data breach notification laws, most existing cyber incident reporting requirements target specific communities with common characteristics. Some focus on entities within a specific industry or sector (e.g., commercial nuclear power reactors; financial services institutions) while others cover entities across sectors that possess certain shared characteristics (e.g., entities possessing threshold quantities of certain chemicals of interest that render those entities high-risk of being targeted by terrorists; entities located upon navigable bodies of water where they present the risk of a transportation security incident; entities that maintain personal health-related records).

Central aspects of cyber incident reporting regimes, such as what constitutes a reportable incident, the process for reporting an incident, which entity receives the report, what information must be reported, and how long an entity has to report the incident, can vary widely from regime to regime, with the purpose of the regime frequently impacting these variables. For instance, reporting regimes focused on national or economic security tend to have shorter deadlines for reporting than those regimes focused on privacy or consumer protections. Similarly, reporting regimes focused on national or economic security almost universally require reporting to a Federal department or agency, while regimes with a primary purpose of privacy or consumer protections often require reporting to the impacted individual and sometimes credit reporting agencies, instead of, or in addition to, reporting to the governing Federal or SLTT entity.

Given the number and variety of different cyber incident reporting regimes, and their continued evolution,

Federal Government at 5 (Sept. 19, 2023), available at <https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government> (hereinafter, “the DHS Report”).

CISA does not intend to describe each one of them as part of this section. Instead, CISA is providing the following brief summaries of some of the major regulatory programs that require reporting of cyber incidents and that are concerned at least in part with national security, economic security, public safety, and/or the resiliency of NCFs:⁵

- *Chemical Facility Anti-Terrorism Standards (CFATS)*. CISA's CFATS program worked for the prior 16 years to identify and regulate high-risk chemical facilities to ensure security measures are in place to reduce the risk of certain chemicals of interest from being weaponized by terrorists. See 6 CFR part 27. Under CFATS Risk-Based Performance Standard 15, CFATS-covered facilities were expected to establish protocols governing the identification and reporting of significant cyber incidents to the appropriate facility personnel, local law enforcement, and/or CISA. On July 28, 2023, the statutory authority for the CFATS program expired, but CISA anticipates that CFATS will be reauthorized prior to the publication of the CIRCIA Final Rule.

- *Defense Federal Acquisition Regulation Supplement (DFARS)*. Pursuant to 32 CFR 236.1–236.7 and 48 CFR 252.204–7012, Department of Defense (DOD) contractors must report to DOD all cyber incidents (1) involving covered defense information on their covered contractor information systems or (2) affecting the contractor's ability to provide operationally critical support. Contractors subject to these requirements, who are members of the Defense Industrial Base sector, must report cyber incidents to DOD at <https://dibnet.dod.mil>.

- *Department of Energy (DOE) DOE-417 reporting requirements*. DOE's Office of Cybersecurity, Energy Security, and Emergency Response requires certain Energy Sector entities to report certain cybersecurity incidents to DOE pursuant to 15 U.S.C. 772(b). Entities subject to the reporting requirements include Balancing Authorities, Reliability Coordinators, some Generating Entities, and Electric Utilities, including those located in Puerto Rico, the Virgin Islands, Guam, or other U.S. possessions.

- *Federal Communications Commission's (FCC) Network Outage Reporting System (NORS) Requirements*. Under 47 CFR part 4,

providers of telecommunications services and Voice over internet Protocol (VoIP) providers are required to report to the FCC communications service outages, including those caused by cyber incidents, that meet certain minimum requirements for duration and magnitude. The goal of this regulation, which applies to wireline, wireless, VoIP, cable, satellite, Signaling System 7, submarine cable, covered 911 service, and covered 988 service providers, is to provide rapid, complete, and accurate information on service disruptions that could affect homeland security, public health or safety, and the economic well-being of the Nation and help ensure the public's access to emergency services.

- *Federal Information Security Modernization Act of 2014*. FISMA requires Federal civilian departments and agencies to report cybersecurity incidents to CISA within one hour of discovery.⁶ CISA uses information received in FISMA incident reports to, among other things, provide technical assistance to victims of cyber incidents, compile and analyze incident information to identify cyber threats and vulnerabilities, and share guidance with others on how to detect, handle, and prevent similar incidents.⁷ Federal agencies are also required to report major incidents under FISMA and pursuant to OMB Guidance, including those that implicate personal information.⁸

- *Federal Risk and Authorization Management Program (FedRAMP)*. FedRAMP requires any cloud service providers (CSPs) with a Federal agency-issued Authority to Operate (ATO) or a FedRAMP-issued provisional ATO to report suspected and confirmed information security incidents to the FedRAMP Program Management Office within the General Services Administration (GSA), CISA, and the affected agency.⁹

- *Financial Services Sector Regulations*. Most of the primary Financial Services Sector regulators have adopted cyber incident reporting requirements for their regulated communities. Among other things, these reporting requirements have been established to help promote early awareness of emerging threats to banking organizations and the broader financial system, and to help the regulating entities react to these threats before they can cause systemic impacts

across the financial system. Included among these are cyber incident reporting requirements managed by the Office of the Comptroller of the Currency (OCC) (12 CFR part 53), the Federal Reserve Board (FRB) (12 CFR part 225), the Federal Deposit Insurance Corporation (FDIC) (12 CFR part 304), the Commodity Futures Trading Commission (CFTC) (see, e.g., 17 CFR 38.1051 (designated contract markets); 17 CFR 37.1401 (swap execution facilities); 17 CFR 39.18 (derivatives clearing organizations); 17 CFR 49.24 (swap data repositories); 17 CFR 23.603 (swap dealers)), the National Credit Union Administration (NCUA) (12 CFR part 748), the Securities and Exchange Commission (SEC) (see, e.g., 17 CFR parts 229, 232, 239, 240, 242, and 249), and the Federal Housing Finance Agency (FHFA) (Advisory Bulletin 2020–05).

- *Maritime Transportation Security Act (MTSA)*. Under MTSA (33 CFR parts 104, 105, or 106) entities that own vessels or facilities, including outer continental shelf facilities, subject to MTSA must report cyber incidents to the U.S. Coast Guard's (USCG) National Response Center. These cyber incident reporting requirements are part of a larger suite of security requirements for vessels and facilities to identify, assess, and prevent transportation security incidents (TSIs) in the marine transportation system. USCG is also in the process of updating its maritime security regulations by adding cybersecurity requirements to existing Maritime Security regulations.¹⁰

- *North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standard CIP-008-6: Cyber Security—Incident Reporting and Response Planning*. Certain electric grid entities, designated as “responsible entities,” are required to report cyber incidents to both CISA and the Electricity Information Sharing and Analysis Center (ISAC), a component of NERC. See 18 CFR part 40 and CIP-008-6. The goal of these reporting requirements, which were developed pursuant to the authority granted NERC in Section 215 of the Federal Power Act (16 U.S.C. Ch 12, as amended through Pub. L. 115–325) to develop mandatory and enforceable reliability standards subject to Federal Energy Regulatory Commission (FERC) review and approval, is to mitigate the risk to the reliable operation of the Bulk Electric

⁵ Individuals interested in learning more about existing Federal cyber incident reporting requirements are encouraged to review the Federal Cyber Incident Reporting Requirements Inventory contained in Appendix B of the *DHS Report*, *supra* note 4.

⁶ 44 U.S.C. 3554(b)(7)(C)(ii).

⁷ 44 U.S.C. 3556(a).

⁸ 44 U.S.C. 3554(b)(7)(C)(iii).

⁹ See *FedRAMP*, GSA, <https://www.gsa.gov/technology/government-it-initiatives/fedramp> (last visited Nov. 27, 2023).

¹⁰ See Office of Management and Budget, *Office of Information and Regulatory Affairs Unified Agenda*, available at <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202304&RIN=1625-AC77>.

System (BES) as the result of a cybersecurity incident.

- *Nuclear Regulatory Commission (NRC) Cyber Security Event Notification Regulation.* Owners and operators of commercial nuclear power reactors are required to report cyber incidents impacting safety, security, or emergency preparedness functions to the NRC.¹¹

- *The Food and Drug Administration (FDA) Medical Device Regulations.* Under section 519 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 360i), as implemented by the Medical Device Reporting Regulations (21 CFR part 803) and the Medical Device Reports of Corrections and Removals Regulations (21 CFR part 806), manufacturers and importers must report certain device-related adverse events and product problems, including those caused by cyber incidents, to the FDA. For example, medical device manufacturers are required to report to the FDA when they learn that any of their devices may have caused or contributed to a death or serious injury. Manufacturers must also report to the FDA when they become aware that their device has malfunctioned and would be likely to cause or contribute to a death or serious injury if the malfunction were to recur. Medical device manufacturers and importers also must report to FDA any correction or removal of a medical device initiated to reduce a risk to health posed by the device or to remedy a violation of the Federal Food, Drug, and Cosmetic Act, including those caused by cyber incidents, caused by the device that may present a risk to health. A report must be made even if the event was caused by user error.

- *Transportation Security Administration (TSA) Security Directives and Security Program Amendments.* TSA has issued several Security Directives and Security Program Amendments requiring various Transportation Systems Sector entities to report cybersecurity incidents to CISA.¹² These include, among other provisions, reporting requirements for certain passenger railroad carrier and rail transit systems, hazardous and natural gas pipeline owners and operators, freight railroad carriers, airport operators, aircraft operators, indirect air carriers, and Certified Cargo Screening Facilities. TSA is also in the process of codifying the requirements for surface transportation through a rulemaking (TSA's regulations provide

for changes to aircraft operator security programs through an amendment process).¹³

C. Purpose of Regulation

While the legislative history and statutory text shed some light on the goals that Congress hoped to achieve through this regulation, Congress did not include an explicit statement of purpose in CIRCIA. CISA believes considering the specific intended purpose behind a cyber incident reporting regulation during the development of the regulations is important as the purpose likely impacts key aspects of the regulation, such as what entities are required to report, what types of incidents must be reported, how quickly incidents must be reported, what information must be included in incident reports, and to whom the reports must be provided.

Many stakeholders echoed this belief in remarks made during CIRCIA listening sessions or through comments provided in response to the CIRCIA RFI, which encouraged CISA to articulate the goals of the regulation to help inform the best regulatory proposal.¹⁴ This section of the NPRM is intended to provide insight into what CISA interprets to be the purposes of the regulation that has informed the development of CISA's proposed regulation.

i. Purposes of the CIRCIA Regulation

CIRCIA's legislative history indicates that the primary purpose of CIRCIA is to help preserve national security, economic security, and public health and safety. For example, in December 2021, HSGAC issued a fact sheet on the proposed legislation acknowledging the "serious national security threat" posed by cyberattacks and stating that CIRCIA would help enable a coordinated,

¹³ See Office of Management and Budget, *Office of Information and Regulatory Affairs Unified Agenda*, available at <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202304&RIN=1652-AA74>.

¹⁴ See 87 FR 55833 (Sept. 12, 2022); comments submitted by Information Technology Industry Council, CISA-2022-0010-0097 ("[I]t is vital that CISA articulate its tactical goals and/or plan for actualizing CIRCIA, as only upon understanding what CISA hopes to accomplish with these reports can industry stakeholders provide more specific commentary on key scoping and reporting threshold questions."); National Grain and Feed Association, CISA-2022-0010-0104 ("CISA should also identify the specific purpose of reporting an incident. For example, if the data will be used by the government for trend identification."); G. Rattray, CISA-2022-0010-0159 ("[CISA] will have to decide whether it is reporting that serves the purpose of characterizing threats or you're trying to understand risks and vulnerability. Both are probably viable analytically, but those would lead to different sort of reporting requirements.").

informed U.S. response to the foreign governments and criminal organizations conducting these attacks against the United States.¹⁵ Similarly, the U.S. House Committee on Homeland Security (CHS) issued a fact sheet on the proposed legislation stating that CIRCIA would provide CISA and its Federal partners the visibility needed to bolster cybersecurity, identify malicious cyber campaigns in early stages, identify longer-term threat trends, and ensure actionable cyber threat intelligence is getting to the first responders and Federal officials who need it.¹⁶

The plain language that Congress used throughout CIRCIA reflects the purpose discussed in CIRCIA's legislative history. For example, CIRCIA requires CISA to review covered cyber incidents that are "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States" and to "identify and disseminate ways to prevent or mitigate similar incidents in the future." 6 U.S.C. 681(9); 6 U.S.C. 681a(a)(6). CIRCIA also requires CISA to "assess potential impact of cyber incidents on public health and safety," and to consider, when describing covered entities, both "the consequences that disruption to or compromise of [a covered entity] could cause to national security, economic security, or public health and safety" and "the extent to which damage, disruption, or unauthorized access to such an entity . . . will likely enable the disruption of the reliable operation of critical infrastructure." 6 U.S.C. 681a(a)(1); 6 U.S.C. 681b(c)(1)(A), 681b(c)(1)(C).

Both CIRCIA's legislative history and statutory text highlight a number of more discrete purposes within the broader goals of enhancing national and economic security, and public health and safety. Some examples of these purposes include trend and threat analysis (*i.e.*, the performance of cybersecurity threat and incident trend analysis and tracking, to include the analysis and identification of adversary tactics, techniques, and procedures (TTPs));¹⁷ vulnerability and mitigation

¹⁵ HSGAC *Fact Sheet*, *supra* note 2, at 1.

¹⁶ CHS, *The Cyber Incident Reporting for Critical Infrastructure Act at 1*, 3 (Aug. 2021), available at <https://democrats-homeland.house.gov/download/incident-reporting-bill-draft-fact-sheet> (hereinafter, "CHS Fact Sheet").

¹⁷ See, *e.g.*, *id.* at 3; *Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021 Before the Subcomm. on Cybersecurity, Infrastructure Protection, and Innovation of the H. Comm. on Homeland Security*,

Continued

¹¹ 10 CFR 73.77.

¹² See, *e.g.*, TSA Security Directive Pipeline-2021-01 series, *Enhancing Pipeline Cybersecurity*; TSA Security Directive 1580-21-01 series, *Enhancing Rail Cybersecurity*, available at <https://www.tsa.gov/sd-and-ea>.

assessment (*i.e.*, the identification of cyber vulnerabilities and the assessment of countermeasures that might be available to address them);¹⁸ the provision of early warnings (*i.e.*, the rapid sharing of information on cyber threats, vulnerabilities, and countermeasures through the issuance of cybersecurity alerts or other means);¹⁹ incident response and mitigation (*i.e.*, rapid identification of significant cybersecurity incidents and offering of assistance—*e.g.*, personnel, services—in incident response, mitigation, or recovery);²⁰ supporting Federal efforts to disrupt threat actors;²¹

117th Cong. 64 (2021), available at <https://www.congress.gov/event/117th-congress/house-event/114018/text> (hereinafter, “Stakeholder Perspectives Hearing”) (statement of Rep. Yvette Clarke) (“One of the goals in drafting this legislation was to provide CISA with enough information to analyze and understand threats”); 6 U.S.C. 681a(a)(1) (CISA must aggregate and analyze reports to identify TTPs adversaries use and to enhance situational awareness of cyber threats across critical infrastructure sectors).

¹⁸ See, *e.g.*, *Responding to and Learning from the Log4Shell Vulnerability Before the S. Comm. on Homeland Security and Governmental Affairs*, 117th Cong. 2 (2022) (statement of Sen. Gary Peters, Chairman, S. Comm. on Homeland Security and Governmental Affairs), available at <https://www.hsgac.senate.gov/hearings/responding-to-and-learning-from-the-log4shell-vulnerability/> (hereinafter, “Log4Shell Vulnerability Hearing Peters Statement”) (“This legislation will help our lead cybersecurity agency better understand the scope of attacks, including from vulnerabilities like Log4j. . . .”); 6 U.S.C. 681a(a)(1) (CISA must aggregate and analyze reports to assess the effectiveness of security controls).

¹⁹ See, *e.g.*, *Log4Shell Vulnerability Hearing Peters Statement*, *supra* note 18, at 2 (“This legislation will help our lead cybersecurity agency . . . warn others of the threat, prepare for potential impacts. . . .”); Minority Staff of S. Comm. on Homeland Security and Governmental Affairs, 117th Cong., *America’s Data Held Hostage: Case Studies in Ransomware Attacks on American Companies* vi (Comm. Print 2022), available at <https://www.hsgac.senate.gov/library/files/americas-data-held-hostage-case-studies-in-ransomware-attacks-on-american-companies/> (“This legislation will enhance the Federal Government’s ability to combat cyberattacks, mount a coordinated defense, hold perpetrators accountable, and prevent and mitigate future attacks through the sharing of timely and actionable threat information.”); 6 U.S.C. 681a(a)(3)(B) (CISA must provide entities with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, cyber threat indicators and defensive measures); 6 U.S.C. 681a(a)(5)–(7) (CISA must identify and disseminate ways to prevent or mitigate cyber incidents, and must review reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to stakeholders).

²⁰ See, *e.g.*, *HSGAC Fact Sheet*, *supra* note 2, at 1 (“This information will allow CISA to provide additional assistance to avoid cyber-attacks against our critical infrastructure, like the attacks on Colonial Pipeline and JBS Foods.”); *Log4Shell Vulnerability Hearing Peters Statement*, *supra* note 18 (“This legislation will help our lead cybersecurity agency . . . help affected entities respond and recover.”).

²¹ See, *e.g.*, Press Release, S. Comm. on Homeland Security and Governmental Affairs, *Portman, Peters*

and advancing cyber resiliency (*i.e.*, developing and sharing strategies for improving overall cybersecurity resiliency; facilitating use of cyber incident data to further cybersecurity research; engagement with software/equipment manufacturers on vulnerabilities and how to close them).²²

ii. How the Regulatory Purpose of CIRCIA Influenced the Design of the Proposed CIRCIA Regulation

Based on CISA’s understanding of the purposes of CIRCIA, CISA identified two fundamental principles that influenced the design of the proposed CIRCIA regulation in key areas. First, to achieve many of the desired goals of the proposed regulation—such as conducting analysis to identify adversary TTPs and providing early warnings to enhance situational awareness of cyber threats across critical infrastructure sectors—CISA needs to receive a sufficient quantity of Covered Cyber Incident Reports and Ransom Payment Reports from across the spectrum of critical infrastructure. As noted by the Cyberspace Solarium Commission, the government’s cyber incident situational awareness, its ability to detect coordinated cyber campaigns, and its cyber risk identification and assessment efforts rely on comprehensive data and, prior to the passage of CIRCIA, the Federal government lacked a mandate to systematically collect cyber incident information reliably and at the scale

Introduce Bipartisan Legislation Requiring Critical Infrastructure Entities to Report Cyberattacks (Sept. 28, 2021), available at <https://www.hsgac.senate.gov/media/dems/peters-and-portman-introduce-bipartisan-legislation-requiring-critical-infrastructure-entities-to-report-cyber-attacks/> (“As cyber and ransomware attacks continue to increase, the federal government must be able to quickly coordinate a response and hold these bad actors accountable.”); Letter from Sen. Rob Portman, Ranking Member, S. Comm. on Homeland Security and Governmental Affairs, to Vanessa Countryman, Secretary, SEC, Re: RE: SEC Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, File No. S7–09–22, 3 (May 9, 2022), available at <https://www.sec.gov/comments/s7-09-22/s70922-20128391-291294.pdf> (“When considering the legislation, Congress noted if the FBI is ‘provided information from reports under the process outlined in the statute, [it] may, as appropriate, use information contained in the reports and derived from them’ for a range of investigatory activities. This is consistent with the statute which states incident reports can be used for ‘the purpose [of] preventing, investigating, disrupting, or prosecuting an offense arising out of a cyber incident’ reported under the law. This allows law enforcement agencies to disrupt and deter hostile cyber actors. . . .” (footnotes omitted)).

²² See, *e.g.*, 6 U.S.C. 681a(a)(9) (CISA must proactively identify opportunities to leverage and utilize data on cyber incidents to enable and strengthen cybersecurity research carried out by academia and private sector organizations).

necessary.²³ Sufficient data also is central to being able to differentiate campaigns from isolated incidents and support the development of more generalizable conclusions.²⁴

If CISA designs the proposed regulations in a way that overly limits the quantity and variety of reports it receives from across critical infrastructure sectors, CISA will lack sufficient information to support reliable trend analysis, vulnerability identification, provision of early warnings, and other key purposes of the proposed regulation as indicated by CIRCIA. This fundamental principle was particularly important for CISA as it considered different options related to which entities should be required to report, what types of cyber incidents should be reported, and the scope and amount of technical detail necessary in CIRCIA Reports to enable CISA to conduct threat analysis, track campaigns, and provide early warnings as required by CIRCIA.

Many stakeholders provided comments in response to the RFI issued in September 2022 cautioning CISA that collecting too many reports could result in data overload and hinder CISA’s ability to identify important trends and vulnerabilities. While CISA agrees that there could be some point at which the number of reports submitted begins to yield diminishing marginal returns, CISA believes that, due to advances in technology and strategies for managing large data sets, the potential challenges associated with receiving large volumes of reports can be mitigated through technological and procedural strategies. Additionally, as discussed in Section IV.E.ii in this document, CISA proposes to design the reporting form in a manner that is easy for a covered entity or third-party submitter to complete, encourages the submission of useful information,

²³ Cyberspace Solarium Commission, *Cyberspace Solarium Commission Report* at 103 (Mar. 2020), available at <https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report/> (hereinafter “*Cyberspace Solarium Commission Report*”); see also Sandra Schmitz-Berndt, “Defining the Reporting Threshold for a Cybersecurity Incident under the NIS Directive and the NIS 2 Directive,” *Journal of Cybersecurity* at 2 (Apr. 5, 2023) (“[L]ow reporting levels result in a flawed picture of the threat landscape, which in turn may impact cybersecurity preparedness.”), available at <https://academic.oup.com/cybersecurity/article/9/1/tyad009/7160387>.

²⁴ See, *e.g.*, CISA, *Cost of a Cyber Incident: Systematic Review and Cross-Validation* at 49 (Oct. 26, 2020) (reliance on limited data sources such as those based on convenience samples “means that no statistical representativeness can be claimed [which] limits the ability to support inference for generalizing results beyond the studied samples.”), available at <https://www.cisa.gov/resources-tools/resources/cost-cyber-incident-systematic-review-and-cross-validation>.

and provides information to CISA in a manner that facilitates analysis and review. As a result, CISA is less concerned about receiving too many reports and more concerned about not receiving enough reports to support the intended regulatory purposes of the CIRCIA regulations. As noted by Microsoft President Brad Smith during his testimony in front of the U.S. Senate Select Committee on Intelligence during a hearing on the “Hack of U.S. Networks by a Foreign Adversary,” in the wake of the supply chain compromise of the SolarWinds Orion product, “one of the challenges in this space is the nature of all threat intelligence, whether it’s cyber-based or physically based, is that it’s always about connecting dots. So the more dots you have, the more likely you are to see a pattern and reach a conclusion. . . . And then they’re spread out across different parts of the public sector as well. So this notion of aggregating them is key.”²⁵

CISA is cognizant of the fact that reporting does not come without costs, however, so CISA is not seeking simply to capture the maximum number of reports possible under the statutory language (*i.e.*, by scoping both the applicability of the rule and covered cyber incidents as broadly as legally permissible). CISA’s goal is to identify and achieve the proper balance among the number of reports being submitted, the benefits resulting from their submission, and the costs to both the reporting entities and the government of the submission, analysis, and storage of those reports.

The second major principle CISA identified that influenced aspects of the proposed regulation was the importance of timeliness in both the receipt of reports and in CISA’s ability to analyze and share information gleaned from those reports. To achieve the very important early visibility and warning aspects of this regulatory regime and increase the likelihood that entities across the critical infrastructure community will be able to address identified vulnerabilities and secure themselves against the latest adversary TTPs before falling victim to them, time is of the essence. CISA kept this second principle in mind as CISA considered options for when a covered entity’s reporting obligations begin under the proposed regulation and the manner, form, and procedures for reporting.

Similar to the first principle, CISA recognizes that potential drawbacks to overprioritizing timely reporting exist, such as potentially impacting a covered entity’s ability to conduct preliminary incident response and mitigation. CISA also recognizes that a covered entity may not have all the information in the early aftermath of incident discovery, and that some preliminary determinations made at the outset of an incident response process may later be determined to be inaccurate when the entity is afforded time to conduct further investigation and analysis. Accordingly, CISA has sought to balance the critical need for timely reporting with the potential challenges associated with rapid reporting in the aftermath of a covered cyber incident. For example, CISA recognizes that covered entities may require some limited time to conduct preliminary analysis before establishing a reasonable belief that a covered cyber incident has occurred and thereby triggering the 72-hour timeframe for reporting. See Section IV.E.iv.1 in this document. Additionally, to the extent that information that is required to be reported under the regulation is evolving or unknown within the initial reporting deadline for a covered cyber incident, CISA is proposing to allow covered entities to submit new or updated information in a Supplemental Report as additional information becomes known about the covered cyber incident. See Section IV.E.iii.4 in this document.

D. Harmonization Efforts

Given the number of existing cyber incident reporting requirements at the Federal and SLTT levels, CISA recognizes that covered entities may be subject to multiple, potentially duplicative requirements to report cyber incidents. In an attempt to minimize the burden on covered entities potentially subject to both CIRCIA and other Federal cyber incident reporting requirements, CISA is committed to exploring ways to harmonize this regulation with other existing Federal reporting regimes, where practicable and seeks comment from the public on how it can further achieve this goal. CISA is already engaged in several efforts in furtherance of harmonization of cyber incident reporting, including: (1) serving as a member of the CIRC and participating in the CIRC’s efforts to coordinate, deconflict, and harmonize Federal cyber incident reporting requirements; (2) participating in the Cybersecurity Forum for Independent and Executive Branch Regulators; (3) performing extensive outreach with

Federal and non-Federal entities to gain a fulsome understanding of the existing cyber incident reporting regulatory landscape and gather perspectives on how to harmonize existing cyber incident reporting requirements; and (4) engaging with other Federal departments and agencies that implement cyber incident reporting requirements to determine whether covered entities could potentially take advantage of the proposed substantially similar reporting exception to CIRCIA reporting (discussed further in Section IV.D.i in this document).

CISA actively participated in the CIRC to help identify potential approaches to harmonizing Federal cyber incident reporting requirements and to support the identification of recommended practices that could be considered by CISA and other Federal departments and agencies as they develop or update their respective cyber incident reporting regimes. Specifically, CISA participated in various DHS-led working groups to identify potential recommended practices and areas of harmonization related to Federal cyber incident reporting requirements, many of which are reflected in the DHS Report.²⁶ CISA considered the DHS Report and its recommendations as it developed this proposed rule and attempted to leverage the model definition and reporting form recommended in the DHS Report to the extent practicable and consistent with the unique regulatory authority granted to CISA under CIRCIA and the purpose of the CIRCIA regulation (described in Sections III.A and C in this document).

CISA has also been an active participant in the Cybersecurity Forum for Independent and Executive Branch Regulators. The goal of this forum, which was initially launched in 2014, is to increase the overall effectiveness and consistency of Federal regulatory authorities related to cybersecurity by enhancing communication among regulatory agencies, sharing best practices, and exploring ways to align, leverage, and deconflict approaches to cybersecurity regulation.²⁷ Current participants in the Forum include, among others, FCC, CISA, CFTC, Consumer Product Safety Commission, Department of Health and Human Services (HHS), DHS, Department of the Treasury, FERC, FHFA, FRB, Federal Trade Commission, FDA, NRC, OCC, SEC, TSA, USCG, and the Office of the National Cyber Director.

²⁶ *DHS Report*, *supra* note 4, at 5.

²⁷ See Cybersecurity Forum for Independent and Executive Branch Regulators Charter (2014), available at <https://www.nrc.gov/docs/ML1501/ML15014A296.pdf>.

²⁵ Testimony of Brad Smith to the U.S. Senate Select Committee on Intelligence, “Hearing on Hack of U.S. Networks by a Foreign Adversary” (Feb. 23, 2021), available at <https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary>.

Additionally, CISA has performed, and as required by CIRCIA, plans on continuing to perform, outreach to both Federal partners and non-Federal stakeholders to learn about existing and proposed cyber incident reporting regulations and ways in which CISA may be able to design and implement the CIRCIA requirements to harmonize with those reporting requirements to the extent practicable. In addition to the RFI and listening sessions described in Section III.F in this document, CISA held a series of consultations with each Sector Risk Management Agency (SRMA), all Federal departments and agencies that currently oversee cyber incident reporting requirements, and various other Federal departments and agencies with equities in cyber incident and ransom payment reporting. During these engagements, CISA has sought to learn about existing and proposed Federal regimes that require the reporting of cyber incidents or ransom payments and discuss areas where CISA and its Federal counterparts might want to, and be able to, harmonize their respective reporting requirements. CISA leveraged the information gained via the RFI, listening sessions, and Federal consultations in the development of this NPRM, and intends to continue to engage Federal partners during the development and implementation of the final rule in an attempt to harmonize reporting requirements and reduce the burden on potential covered entities, where practicable.

Finally, CISA intends to work with other Federal departments and agencies to explore opportunities to reduce duplicative reporting of covered cyber incidents through a proposed substantially similar reporting exception to CIRCIA. Under this exception, which is authorized under 6 U.S.C. 681b(a)(5)(B), a covered entity that is required by law, regulation, or contract to report information to another Federal entity that is substantially similar to the information that must be reported under CIRCIA and is required to submit the report in a substantially similar timeframe to CIRCIA's reporting deadlines, may be excepted from reporting it again under CIRCIA. Per the statute, for covered entities to be able to leverage this specific exception, CISA and the respective Federal entity must enter into an interagency agreement, referred to as a CIRCIA Agreement, and establish an information sharing mechanism to share reports. To the extent practicable, CISA is committed to working in good faith with its Federal partners to have CIRCIA Agreements finalized before the effective date of the

final rule. Additional details on the substantially similar reporting exception to CIRCIA are discussed in Section IV.D.i in this document.

CISA welcomes all comments on all aspects of harmonizing CIRCIA's regulatory reporting requirements with other cyber incident and ransom payment reporting requirements, including:

1. Potential approaches to harmonizing CIRCIA's regulatory reporting requirements with other existing Federal or SLTT laws, regulations, directives, or similar policies that require reporting of cyber incidents or ransom payments.

2. How to reduce actual, likely, or potential duplication or conflict between other Federal or SLTT laws, regulations, directives, or policies and CIRCIA's reporting requirements.

E. Information Sharing Required by CIRCIA

Sharing information on cyber incidents, ransomware attacks, and the broader cyber threat landscape is central to CIRCIA. In fact, CIRCIA imposes several requirements upon CISA and other Federal departments and agencies related to the sharing of information received through cyber incident and ransom payment reporting programs, including the CIRCIA proposed regulations. As Congress imposed these obligations solely on Federal departments and agencies, they are not included in the CIRCIA proposed rule; however, information sharing will be an integral part of the overall CIRCIA implementation, and CISA is committed to working with its Federal partners to share cyber threat information across the Federal government and, as appropriate, with non-Federal stakeholders.

As required by 6 U.S.C. 681a(a)(10) and (b), CISA will make information received via CIRCIA Reports or in response to an RFI or subpoena available to appropriate SRMAs and other appropriate Federal departments and agencies, as determined by the President or a designee of the President, within 24 hours of receipt. CIRCIA also includes a reciprocal requirement, where any Federal department or agency that receives a report of a cyber incident shall provide the report to CISA within 24 hours of receiving the report. See 6 U.S.C. 681g(a)(1). Upon receipt of a report from another Federal agency pursuant to this requirement, CISA must share the report with other Federal agencies as it would any other report submitted to CISA under CIRCIA. 6 U.S.C. 681a(a)(10), 681a(b), 681g(a)(1). In addition to any otherwise generally

applicable laws (such as the Privacy Act of 1974²⁸ and the E-Government Act of 2002²⁹), pursuant to 6 U.S.C. 681g(a)(3), CISA must protect the reports it receives from Federal partners under these provisions in accordance with any privacy, confidentiality, or information security requirements imposed upon the originating Federal department or agency. CIRCIA also requires CISA to “coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments.” 6 U.S.C. 681a(a)(2).

CIRCIA imposes requirements on CISA related to sharing cyber threat information with non-Federal stakeholders as well. For example, 6 U.S.C. 681a(a)(7) requires CISA to immediately review Covered Cyber Incident Reports or voluntary reports submitted to CISA pursuant to 6 U.S.C. 681c to the extent they involve ongoing cyber threats or security vulnerabilities for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders. Similarly, for a covered cyber incident or group of covered cyber incidents that satisfies the definition of a significant cyber incident, CISA must conduct a review of the details surrounding the incident(s) and identify and disseminate ways to prevent or mitigate similar incidents in the future. 6 U.S.C. 681a(a)(6). CISA must also “publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations” based on Covered Cyber Incident Reports. 6 U.S.C. 681a(a)(8). In addition to limiting sharing of information as may otherwise be required by laws that are generally applicable to information received by the Federal government, such as the Trade Secrets Act,³⁰ when sharing with critical infrastructure owners and operators and the general public any information received via CIRCIA Reports or responses to RFIs, CISA must anonymize information related to the victim who reported the incident. See 6 U.S.C. 681e(d).

F. Summary of Stakeholder Comments

While developing this NPRM, CISA sought feedback from an array of public and private sector stakeholders in an effort to identify the most effective potential approach to implementing CIRCIA's reporting requirements. CISA published an RFI in the **Federal**

²⁸ See 5 U.S.C. 552a.

²⁹ See 44 U.S.C. 3501 note, Public Law 107–347.

³⁰ 18 U.S.C. 1905.

Register; ³¹ held in-person, public listening sessions around the country; ³² conducted virtual, sector-specific listening sessions; ³³ and consulted with SRMAs and other relevant Federal departments and agencies, all with the goal of receiving meaningful input from entities that will potentially be impacted by this regulation. CISA has considered this feedback when developing the proposals set forth in this NPRM. A summary of the most salient points received in response to the RFI and during the CIRCIA listening sessions follows. All comments received in response to the RFI, as well as transcripts from all the public and sector-specific listening sessions, are available in the electronic docket for this rulemaking.

i. General Comments

In general, several commenters told CISA that the regulations should be easy to comply with, such that individuals who are not cybersecurity professionals can complete the required reporting, and avoid overly burdensome requirements. ³⁴ Commenters recommended that compliance with the regulation be incentive-based and

supportive, rather than punitive, ³⁵ and commenters also expressed concerns about the confidentiality of reported information. ³⁶ Commenters also urged CISA to consider the landscape of existing cyber incident reporting requirements and expressed general concern about the potential negative impacts of unharmonized, complex, and duplicative reporting regimes. ³⁷

ii. Comments on the Definition of Covered Entity

Several commenters provided suggestions on how to define the term covered entity under this regulation. While some commenters thought the definition of covered entity was straightforward and already understood, ³⁸ others pointed to different criteria or frameworks CISA could use to scope the definition more effectively. These included, among others, a size-based threshold, ³⁹ a risk-based approach, ⁴⁰ or a focus on the degree to which an entity supported a NCF. ⁴¹ Commenters also suggested leveraging existing lists, standards, or definitions, such as the list of critical infrastructure “where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security,” as determined pursuant to Section 9(a) of Executive Order 13636; ⁴² the NERC CIP standard; ⁴³ the National Institute of Standards and Technology’s (NIST’s)

definition; ⁴⁴ or definitions used by other countries. ⁴⁵ Others suggested considering the unique qualities of particular industries and sectors and either creating sector-based definitions or excluding certain sectors and industries from the definition altogether. ⁴⁶

iii. Comments on the Definition of Covered Cyber Incident and Substantial Cyber Incident

Many commenters provided thoughts on how to define covered cyber incident and substantial cyber incident, including some who offered their own definitions for CISA to consider. ⁴⁷ Multiple commenters indicated a desire for a high threshold for reporting to minimize burdens on regulated entities, avoid duplicative reporting, and prevent CISA from being inundated with reports, ⁴⁸ although at least one commenter noted that a narrow definition could leave CISA with an incomplete understanding of the threat landscape. ⁴⁹ In recommending high thresholds, commenters suggested that CISA could bound the definition of covered cyber incident in a variety of ways, such as by limiting reporting to “confirmed incidents”; ⁵⁰ incidents that cause “actual harm”; ⁵¹ only incidents that impact business operations; ⁵² only

³¹ The RFI, which was published in the **Federal Register** on September 12, 2022, solicited inputs on potential aspects of the proposed regulation prior to the publication of this NPRM. CISA did not limit the type of feedback commenters could submit in response to the RFI, but did specifically request comments on definitions for and interpretations of the terminology to be used in the proposed regulation; the form, manner, content, and procedures for submission of reports required under CIRCIA; information regarding other incident reporting requirements including the requirement to report a description of the vulnerabilities exploited; and other policies and procedures, such as enforcement procedures and information protection policies, that will be required for implementation of the regulation. The comment period was open through November 14, 2022, and CISA received 131 individual comments in response to the RFI. 87 FR 55833.

³² Between September 21, 2022, and November 16, 2022, CISA hosted ten listening sessions in Salt Lake City, Utah; Chicago, Illinois; Fort Worth, Texas; New York, New York; Philadelphia, Pennsylvania; Washington, DC; Oakland, California; Boston, Massachusetts; Seattle, Washington; and Kansas City, Missouri. 87 FR 55830; 87 FR 60409.

³³ Because CIRCIA defines covered entities with reference to critical infrastructure sectors, CISA held sector-specific listening sessions for each of the 16 critical infrastructure sectors identified in Presidential Policy Directive 21, see <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>, as well as a separate session for the Aviation Subsector. Transcripts from these sessions can be viewed in the docket for this rulemaking by going to www.regulations.gov and searching for CISA–2022–0010.

³⁴ See, e.g., Comments submitted by the Confidentiality Coalition, CISA–2022–0010–0030; Credit Union National Association, CISA–2022–0010–0050; SAP, CISA–2022–0010–0114; Federation of American Hospitals, CISA–2022–0010–0063; Epic, CISA–2022–0010–0090.

³⁵ See, e.g., Comments submitted by the Arizona Cyber Threat Response Alliance and Arizona Technical Council, CISA–2022–0010–0022; SolarWinds, CISA–2022–0010–0027.

³⁶ See, e.g., Comments submitted by Google Cloud, CISA–2022–0010–0109; Tenable, CISA–2022–0010–0032; NCTA—The Internet & Television Association, CISA–2022–0010–0102.

³⁷ See, e.g., Comments submitted by CTIA, CISA–2022–0010–0070; R Street Institute, CISA–2022–0010–0125; IBM, CISA–2022–0010–0069; Cybersecurity Coalition, CISA–2022–0010–0105.

³⁸ See, e.g., Comment submitted by the Arizona Cyber Threat Response Alliance and Arizona Technical Council, CISA–2022–0010–0022.

³⁹ See, e.g., Comments submitted by the Computing Technology Industry Association, CISA–2022–0010–0122; BlackBerry Corporation, CISA–2022–0010–0036; Cyber Threat Alliance, CISA–2022–0010–0019; SolarWinds, CISA–2022–0010–0027.

⁴⁰ See, e.g., Comments submitted by the Information Technology Industry Council, CISA–2022–0010–0097; U.S. Chamber of Commerce, CISA–2022–0010–0075; American Property Casualty Insurance Association, CISA–2022–0010–0064.

⁴¹ See, e.g., Comment submitted by Mitchell Berger, CISA–2022–0010–0004.

⁴² See, e.g., Comments submitted by the UnityPoint Health, CISA–2022–0010–0107; National Retail Federation, CISA–2022–0010–0092; National Rural Electric Cooperative Association, CISA–2022–0010–0025.

⁴³ See, e.g., Comment submitted by the Powder River Energy Corporation, CISA–2022–0010–0099.

⁴⁴ See, e.g., Comment submitted by the Credit Union National Association, CISA–2022–0010–0050.

⁴⁵ See, e.g., Comment submitted by SAP, CISA–2022–0010–0114.

⁴⁶ See, e.g., Comments submitted by the Rural Wireless Association, Inc., CISA–2022–0010–0093 (recommending excluding small telecommunications carriers); TechNet, CISA–2022–0010–0072 (discussing the “innovation economy”); American Property Casualty Insurance Association, CISA–2022–0010–0064 (recommending exclusion of insurance agencies); NAFCU, CISA–2022–0010–0076 (recommending exclusion of the credit union industry).

⁴⁷ See, e.g., Comments submitted by the Cybersecurity Coalition, CISA–2022–0010–0105; Microsoft Corporation, CISA–2022–0010–0058.

⁴⁸ See, e.g., Comments submitted by The Associations: BPI, ABA, IIB, SIFMA, CISA–2022–0010–0046; American Council of Life Insurers, CISA–2022–0010–0095; UnityPoint Health, CISA–2022–0010–0107; Cloudflare, Inc., CISA–2022–0010–0074; American Property Casualty Insurance Association, CISA–2022–0010–0064; Jim Wollbrinck, CISA–2022–0010–0151.

⁴⁹ See, e.g., Comment submitted by NERC, CISA–2022–0010–0049.

⁵⁰ See, e.g., Comments submitted by Mandiant, CISA–2022–0010–0120; Edison Electric Institute, CISA–2022–0010–0079; Connected Health Initiative, CISA–2022–0010–0130; ACT | The App Association, CISA–2022–0010–0129.

⁵¹ See, e.g., Comments submitted by the internet Infrastructure Coalition, CISA–2022–0010–0055; Independent Community Bankers of America, CISA–2022–0010–0080; Institute of International Finance, CISA–2022–0010–0060.

⁵² See, e.g., Comments submitted by IBM, CISA–2022–0010–0069; Edison Electric Institute, CISA–

incidents that impact an entity's critical infrastructure functions;⁵³ incidents that directly impact U.S. companies, citizens, economies or national security;⁵⁴ and/or those resulting only from malicious intent.⁵⁵ Several commenters also advocated for considering definitions that already exist, such as the definition created by NIST that is used in FISMA,⁵⁶ or definitions that are already used among the 16 critical infrastructure sectors.⁵⁷

Comments received on the potential definition of substantial cyber incident echoed those received on the potential definition of covered cyber incident, though a few commenters noted that the term substantial cyber incident does not have existing legal definitions as does covered cyber incident.⁵⁸ One commenter noted that CISA should

2022-0010-0079; Fidelity National Information Services, CISA-2022-0010-0033; National Technology Security Coalition, CISA-2022-0010-0061.

⁵³ See, e.g., Comments submitted by IBM, CISA-2022-0010-0069; CrowdStrike, CISA-2022-0010-0128; Microsoft Corporation, CISA-2022-0010-0058; Professional Services Council, CISA-2022-0010-0044; Alliance for Automotive Innovation (Auto Innovators), CISA-2022-0010-0082; Telecommunications Industry Association, CISA-2022-0010-0132.

⁵⁴ See, e.g., Comments submitted by Airlines for America, CISA-2022-0010-0066; U.S. Chamber of Commerce, CISA-2022-0010-0075; Express Association of America, CISA-2022-0010-0038; The Associations: AFPM, AGA, API, APGA, INGAA, LEPA, CISA-2022-0010-0057.

⁵⁵ See, e.g., Comments submitted by Cloudflare, Inc., CISA-2022-0010-0074; The Associations: BPI, ABA, IIB, SIFMA, CISA-2022-0010-0046; internet Infrastructure Coalition, CISA-2022-0010-0055.

⁵⁶ See, e.g., Comments submitted by the National Technology Security Coalition, CISA-2022-0010-0061; The Associations: BPI, ABA, IIB, SIFMA, CISA-2022-0010-0046; Mandiant, CISA-2022-0010-0120; Glenn Herdrich, CISA-2022-0010-0158.

⁵⁷ See, e.g., Comments submitted by NCTA—The Internet & Television Association, CISA-2022-0010-0102 (generally advocating for a sector-based approach to the definition); Financial Services Sector Coordinating Council, CISA-2022-0010-0094; The Associations: BPI, ABA, IIB, SIFMA, CISA-2022-0010-0046; The Clearing House, CISA-2022-0010-0086 (advocating for alignment with the FDIC's Computer-Security Incident Notification Rule); HIMSS Electronic Health Record Association, CISA-2022-0010-0040 (advocating for alignment with the Health Insurance Portability and Accountability Act requirements); Nuclear Energy Institute, CISA-2022-0010-0029; Rich Mogavero, CISA-2022-0010-0139 (advocating alignment with the definition used by the NRC); Electric Power Supply Association, CISA-2022-0010-0045; Edison Electric Institute, CISA-2022-0010-0079 (advocating for alignment with the reporting standards used by the NERC); NTCA—The Rural Broadband Association, CISA-2022-0010-0100 (recommending consideration of the FCC's reporting requirements in developing the definition).

⁵⁸ See, e.g., Comments submitted by the Association of Metropolitan Water Agencies, CISA-2022-0010-0088; U.S. Chamber of Commerce, CISA-2022-0010-0075; Fidelity National Information Services, CISA-2022-0010-0033.

clarify whether “substantial cyber incidents” are separate from “covered cyber incidents,”⁵⁹ and another commenter recommended covered cyber incidents and substantial cyber incidents should be synonymous terms.⁶⁰

iv. Comments on Other Definitions

CISA received a small number of comments on other definitions. A few commenters provided feedback on the meaning of the terms ransom payment and ransomware attack, with several noting that the definitions of ransom payment and ransomware attack were understood as defined in CIRCIA and recommending no changes to these terms in the regulation.⁶¹

A few commenters offered input on the meaning of supply chain compromise, with those who did often acknowledging the statutory definition of the term (see 6 U.S.C. 650(28)),⁶² and recommending that CISA align this term as closely as possible with similar, existing terms, such as “supply chain attack” used by NIST or the definition of “supply chain compromise” used by MITRE.⁶³ Several commenters emphasized a need for clarity regarding when a customer or end user would be expected to report on an incident caused somewhere above them in the supply chain, noting that in many cases the impacted covered entity may have limited visibility into what happened along the supply chain to cause the incident.⁶⁴

v. Comments on Criteria for Determining Whether the Domain Name System Exception Applies

The few comments received relating to whether an entity is a multi-stakeholder organization that develops, implements, and enforces policies concerning the DNS reflected different views. One commenter recommended that CISA clarify that domain name registries and registrars are “governed

⁵⁹ See, e.g., Comment submitted by the Professional Services Council, CISA-2022-0010-0044.

⁶⁰ See, e.g., Comment submitted by Gideon Rasmussen, CISA-2022-0010-0011.

⁶¹ See, e.g., Comments submitted by (ISC)2, CISA-2022-0010-0112; Exelon Corp., CISA-2022-0010-0043; SAP, CISA-2022-0010-0114.

⁶² See, e.g., Comment submitted by the Cybersecurity Coalition, CISA-2022-0010-0105.

⁶³ See *id.*; see, e.g., Comment submitted by the Information Technology Industry Council, CISA-2022-0010-0097.

⁶⁴ See, e.g., Comments submitted by the American Water Works Association, CISA-2022-0010-0127; Edison Electric Institute, CISA-2022-0010-0079; NCTA—The Internet & Television Association, CISA-2022-0010-0102; Exelon Corp., CISA-2022-0010-0043.

by a multistakeholder organization.”⁶⁵ Another commenter opined that it would not be appropriate to exempt domain name registrars. The same commenter recommended that CISA identify exempted organizations by name in the final rule, listing Internet Corporation for Assigned Names and Numbers (ICANN) and the Regional Internet Registries for consideration.⁶⁶

vi. Comments on Manner and Form of Reporting, Content of Reports, and Reporting Procedures

Numerous commenters provided recommendations on the manner and form of reporting, with many of those concurring with the use of a web-based form for reporting or other means of electronic reporting.⁶⁷ Some explicitly recommended that CISA make a mobile application or otherwise make the form available via a mobile device as well.⁶⁸ Several commenters recommended alternative or additional methods of reporting to include phone or email.⁶⁹ Multiple commenters emphasized that reporting should not require the download or purchase of new technology.⁷⁰ A number of commenters recommended that the same portal be used for Supplemental Reports as for the original reports.⁷¹

Overall, commenters emphasized the need for a user-friendly reporting form. While several commenters recommended that the reporting form be

⁶⁵ Comment submitted by the Internet Infrastructure Coalition, CISA-2022-0010-0055.

⁶⁶ See Comment submitted by the Energy Transfer LP, CISA-2022-0010-0037. Regional Internet Registries include ARIN, LACNIC, RIPE NCC, AFRINIC, and APNIC (see Regional Internet Registries | The Number Resource Organization (nro.net)).

⁶⁷ See, e.g., Comments submitted by American Council of Life Insurers, CISA-2022-0010-0095; HIMSS Electronic Health Record Association, CISA-2022-0010-0040; Epic, CISA-2022-0010-0090; Cyber Threat Alliance, CISA-2022-0010-0019; League of Southeastern Credit Unions, CISA-2022-0010-0121; Marty Reynolds, CISA-2022-0010-0135; Patrick Thornton, CISA-2022-0010-0144.

⁶⁸ See, e.g., Comments submitted by the Cyber Threat Alliance, CISA-2022-0010-0019; Workgroup for Electronic Data Interchange, CISA-2022-0010-0041; OCHIN, CISA-2022-0010-0039; Cybersecurity Coalition, CISA-2022-0010-0105.

⁶⁹ See, e.g., Comments submitted by CHIME, CISA-2022-0010-0035; Business Roundtable, CISA-2022-0010-0115; CTIA, CISA-2022-0010-0070; The Clearing House, CISA-2022-0010-0086.

⁷⁰ See, e.g., Comments submitted by the Operational Technology Cybersecurity Coalition, CISA-2022-0010-0108; NTCA—The Rural Broadband Association, CISA-2022-0010-0100; Tenable, CISA-2022-0010-0032.

⁷¹ See, e.g., Comments submitted by the Cybersecurity Coalition, CISA-2022-0010-0105; Information Technology Industry Council, CISA-2022-0010-0097; Credit Union National Association, CISA-2022-0010-0050.

standardized for all covered entities,⁷² at least one commenter noted that a uniform reporting format could unintentionally limit the type of information CISA receives.⁷³ Many commenters recommended that any reporting form include drop-down menus, check-boxes, or other fields that could be pre-populated for ease of submission.⁷⁴ Other commenters recommended that the incident reporting form generate questions pertinent to the type of incident being reported, including an indication of which fields were required for each type of report.⁷⁵ Several commenters also recommended that CISA assign reference numbers to each report, which would allow entities to more easily locate and return to a specific CIRCIA Incident Reporting Form at a later point.⁷⁶ Commenters also recommended existing reporting or submission procedures that CISA could emulate. Some commenters recommended CISA rely on a standardized approach, noting examples such as the National Information Exchange Model⁷⁷ or Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII).⁷⁸ Other commenters recommended CISA align its reporting approach to that of other

Federal departments and agencies such as USCG,⁷⁹ TSA,⁸⁰ or DOD.⁸¹

When proposing suggestions for the content of CIRCIA reports, many commenters recommended that CISA require minimal detail at the 72-hour reporting deadline to not divert resources from response efforts,⁸² emphasizing that covered entities should be required to report only what is absolutely needed.⁸³ Several commenters recommended a core set of questions be asked for every covered entity,⁸⁴ while others suggested the question set could be sector-specific.⁸⁵ Many commenters offered their thoughts on specific pieces of data that CISA should consider collecting via the CIRCIA reporting form, many, if not most, of which covered entities are statutorily required to include in either Covered Cyber Incident Reports or Ransom Payment Reports.⁸⁶ Some non-

statutorily required fields that commenters suggested included: identification of critical infrastructure sector, anyone else that the entity informed, severity of the event, and victim IP addresses.⁸⁷

vii. Comments on the Deadlines for Submission of CIRCIA Reports

Although the 72-hour reporting deadline for the reporting of a covered cyber incident is codified in the text of CIRCIA itself, several commenters offered thoughts on how to interpret this requirement. Many commenters suggested that CISA provide flexibility in initiating the 72-hour clock due to the challenges entities face in identifying a “reasonable belief” and responding to covered cyber incidents.⁸⁸ Similarly, commenters urged that CISA adopt certain flexibilities in considering the deadline to have been met, such as allowing entities to omit fields on a form when information is not yet known⁸⁹ or provide extensions to the 72-hour deadline when covered entities are experiencing an external event, such as a natural disaster or pandemic.⁹⁰ A few commenters noted that it may not be objective or clear in the moment when a covered entity has a “reasonable belief,” and recommended that CISA consider determining whether a reasonable belief exists on a case-by-case basis.⁹¹ Many commenters stated that “reasonable belief” should be defined as a confirmed or validated

⁷² See, e.g., Comments submitted by the Alliance for Automotive Innovation, CISA–2022–0010–0082; Lucid Motors, CISA–2022–0010–0078; USTelecom—The Broadband Association, CISA–2022–0010–0067; Palo Alto Networks, CISA–2022–0010–0089.

⁷³ See, e.g., Comment submitted by the Association of American Railroads, CISA–2022–0010–0117.

⁷⁴ See, e.g., Comments submitted by the Workgroup for Electronic Data Interchange, CISA–2022–0010–0041; CTIA, CISA–2022–0010–0070; Anonymous, CISA–2022–0010–0012; National Grain and Feed Association, CISA–2022–0010–0104; Mitchell Berger, CISA–2022–0010–0004; League of Southeastern Credit Unions, CISA–2022–0010–0121; NERC, CISA–2022–0010–0049.

⁷⁵ See, e.g., Comments submitted by the Municipal Information Systems Association of California, CISA–2022–0010–0118; City of Roseville, CISA–2022–0010–0111; City of Cerritos, CISA–2022–0010–0084; Cyber Threat Alliance, CISA–2022–0010–0019; (ISC)2, CISA–2022–0010–0112.

⁷⁶ See, e.g., Comments submitted by the Arizona Cyber Threat Response Alliance and Arizona Technical Council, CISA–2022–0010–0022; Workgroup for Electronic Data Interchange, CISA–2022–0010–0041.

⁷⁷ See, e.g., Comments submitted by the Cyber Threat Alliance, CISA–2022–0010–0019; SolarWinds, CISA–2022–0010–0027; MITRE, CISA–2022–0010–0073.

⁷⁸ See, e.g., Comments submitted by ACT | The App Association, CISA–2022–0010–0129; Connected Health Initiative, CISA–2022–0010–0130; Cyber Threat Alliance, CISA–2022–0010–0019; HIMSS, CISA–2022–0010–0119.

⁷⁹ See, e.g., Comment submitted by the American Association of Port Authorities, CISA–2022–0010–0126.

⁸⁰ See, e.g., Comment submitted by Energy Transfer LP, CISA–2022–0010–0037.

⁸¹ See, e.g., Comment submitted by Trustwave Government Solutions, CISA–2022–0010–0096.

⁸² See, e.g., Comments submitted by BSA | The Software Alliance, CISA–2022–0010–0106; SAP, CISA–2022–0010–0114; Arizona Cyber Threat Response Alliance and Arizona Technical Council, CISA–2022–0010–0022; American Chemistry Council, CISA–2022–0010–0098; U.S. Chamber of Commerce, CISA–2022–0010–0075.

⁸³ See, e.g., Comments submitted by CHIME, CISA–2022–0010–0035; Google Cloud, CISA–2022–0010–0109; The Clearing House, CISA–2022–0010–0086; Information Technology-ISAC, CISA–2022–0010–0048.

⁸⁴ See, e.g., Comments submitted by the Institute of International Finance, CISA–2022–0010–0060; National Association of Chemical Distributors, CISA–2022–0010–0056; UnityPoint Health, CISA–2022–0010–0107; Powder River Energy Corporation, CISA–2022–0010–0099.

⁸⁵ See, e.g., Comments submitted by HIMSS, CISA–2022–0010–0109; CHIME, CISA–2022–0010–0035; CTIA, CISA–2022–0010–0070.

⁸⁶ See, e.g., Comments submitted by the U.S. Chamber of Commerce, CISA–2022–0010–0075 (recommending that CISA focus on the ten elements listed in CISA’s *Sharing Cyber Event Information: Observe, Act, Report* document, namely: incident date and time, incident location, type of observed activity; detailed narrative of the event; number of people or systems affected; company/organization name; point of contact details; severity of event; critical infrastructure sector; and anyone else the entity informed.); Cyber Threat Alliance, CISA–2022–0010–0019 (recommending that the form include three “layers,” containing fields applicable to all incidents (victim information, incident type, incident information, and threat actor information), incident specific fields (with different fields each for business email compromise, ransomware or other extortion, data theft, financial theft such as banking trojans, service theft, denial of service, disruptive or destructive attack, data manipulation or integrity loss, branding/reputation attack, or unauthorized access), and an optional layer for the provision of technical information (such as victim IP addresses, threat actor groups, MITRE ATT&CK mapping, exploited vulnerabilities)); Municipal Information Systems Association of California, CISA–2022–0010–0118 (recommending that the

form include impacted “[a]gency,” date of incident, date incident discovered, indicators of compromise, type of data compromised (if applicable), other compliance agencies mandated to receive this report, a description of the incident, steps taken so far, and logs); City of Roseville, CISA–2022–0010–0111 (same); City of Cerritos, CISA–2022–0010–0084 (same); Palo Alto Networks, CISA–2022–0010–0089 (recommending that the template reporting form include the attack vector or vectors that led to the compromise; tactics or techniques used by threat actor; indicators of compromise; information on the affected systems, devices, or networks; information relevant to the identification of the threat actor or actors involved; a point of contact from the affected entity; and impact, earliest known time, and duration of compromise); Mitchell Berger, CISA–2022–0010–0004 (suggesting that CISA include a list of the 16 critical infrastructure sectors, 55 national critical functions, or similar items with boxes to check).

⁸⁷ See *id.*

⁸⁸ See, e.g., Comments submitted by Cybersecurity Coalition, CISA–2022–0010–0105; TechNet, CISA–2022–0010–0072; Federation of American Hospitals, CISA–2022–0010–0063; National Association of Manufacturers, CISA–2022–0010–0087; American Council of Life Insurers, CISA–2022–0010–0095.

⁸⁹ See, e.g., Comment submitted by Google Cloud, CISA–2022–0010–0109.

⁹⁰ See, e.g., Comment submitted by HIMSS, CISA–2022–0010–0119.

⁹¹ See, e.g., Comments submitted by NCTA—The Internet & Television Association, CISA–2022–0010–0102; SAP, CISA–2022–0010–0114; CTIA, CISA–2022–0010–0070.

cyber incident from the perspective of the covered entity and that the 72-hour clock should therefore begin at that time.⁹²

Similarly, several commenters recommended specific interpretations for the point at which the 24-hour clock deadline for submission of a Ransom Payment Report should begin. For instance, commenters recommended that the 24-hour clock should begin after the ransom payment is sent,⁹³ when “funds or items of value are transmitted to the extorting party,”⁹⁴ or as soon as “any part” of the ransom payment is no longer in possession of the impacted entity or any of its affiliated third parties.⁹⁵

In regards to Supplemental Reports, while some commenters recommended flexibility, including no deadline for timing of submission of Supplemental Reports,⁹⁶ others recommended CISA provide a separate deadline for the submission of Supplemental Reports.⁹⁷ Recommended deadlines varied from as short as 12 hours after discovering substantially new or different information⁹⁸ to as long as one year after the incident.⁹⁹ On the question of what should constitute substantially new or different information that would necessitate filing a Supplemental Report, many commenters recommended that covered entities be permitted to decide when new findings necessitate a Supplemental Report.¹⁰⁰ Other commenters suggested the types

of material changes that could be considered substantial new or different information, such as changes to the types of data stolen or altered; changes to the number or type of systems impacted; or updates to information regarding the TTPs used in the incident.¹⁰¹

viii. Comments on Third-Party Submitters

Of the commenters who offered feedback on the third-party submissions of CIRCIA Reports, most seemed to support the framework already contemplated by statute. For instance, one commenter stated that organizations should be able to identify a third party to submit on their behalf,¹⁰² and more than one stated that the reporting mechanisms, guidelines, and procedures should be the same for the third-party submitter as for the covered entity.¹⁰³ Many commenters recommend that CISA clarify that the duty to comply with the regulation falls on the covered entity,¹⁰⁴ and that third-party submitters have no obligation to report on the covered entity’s behalf.¹⁰⁵

Some commenters recommended additional safeguards for covered entities using third-party reporters. A few commenters recommended that CISA clarify the types of third parties authorized to submit reports on behalf of the covered entity.¹⁰⁶ One commenter recommended that CISA consider entities like ISACs to be suitable third-party reporters.¹⁰⁷ Multiple commenters also recommended that CISA allow third-party submitters to register with

CISA as a known third-party submitter.¹⁰⁸

ix. Comments on Data and Records Preservation Requirements

Very few commenters offered recommendations related to data and records preservation requirements. Several of those that did recommended CISA not impose additional data and records preservation requirements on covered entities via the CIRCIA regulation, and instead defer to covered entities’ existing legal obligations or specific requests from law enforcement.¹⁰⁹ Only one commenter offered suggestions on the type of information that covered entities should preserve,¹¹⁰ while a small number of commenters recommended lengths of time for how long CISA should require information to be preserved.¹¹¹

x. Comments on Other Existing Cyber Incident Reporting Requirements and the Substantially Similar Reporting Exception

Many commenters offered feedback on the breadth of existing Federal, SLTT, and international cyber incident reporting requirements, and the potential for overlap, conflict, or alignment between CIRCIA and those requirements. CISA will not summarize the specific reporting requirements that commenters mentioned, because CISA provides a high-level summary of these existing reporting requirements in Section III.B in this document.

To avoid duplicative and burdensome reporting, several commenters recommended that CISA align its reporting requirements with existing Federal and SLTT requirements.¹¹²

⁹² See, e.g., Comments submitted by National Electrical Manufacturers Association, CISA–2022–0010–0026; League of Southeastern Credit Unions, CISA–2022–0010–0121; The Associations: AFPM, AGA, API, APGA, INGAA, LEPA, CISA–2022–0010–0057; Trustwave Government Solutions, CISA–2022–0010–0096; Microsoft Corporation, CISA–2022–0010–0058.

⁹³ See, e.g., Comments submitted by Exelon Corp., CISA–2022–0010–0043; Cybersecurity Coalition, CISA–2022–0010–0105; Credit Union National Association, CISA–2022–0010–0050; National Association of Chemical Distributors, CISA–2022–0010–0056.

⁹⁴ See, e.g., Comment submitted by the Cybersecurity Coalition, CISA–2022–0010–0105.

⁹⁵ See, e.g., Comment submitted by Sophos, Inc, CISA–2022–0010–0047.

⁹⁶ See, e.g., Comments submitted by the Airlines for America, CISA–2022–0010–0066; SAP, CISA–2022–0010–0114.

⁹⁷ See, e.g., Comments submitted by SolarWinds, CISA–2022–0010–0027; Workgroup for Electronic Data Interchange, CISA–2022–0010–0041; Telecommunications Industry Association, CISA–2022–0010–0132.

⁹⁸ See, e.g., Comment submitted by Sophos, Inc, CISA–2022–0010–0047.

⁹⁹ See, e.g., Comment submitted by the Workgroup for Electronic Data Interchange, CISA–2022–0010–0041.

¹⁰⁰ See, e.g., Comments submitted by USTelecom—The Broadband Association, CISA–2022–0010–0067; Institute of International Finance, CISA–2022–0010–0060; Exelon Corp., CISA–2022–0010–0043.

¹⁰¹ See, e.g., Comments submitted by the Institute of International Finance, CISA–2022–0010–0060; League of Southeastern Credit Unions, CISA–2022–0010–0121; Payments Leadership Council, CISA–2022–0010–0031.

¹⁰² See, e.g., Comment submitted by American Chemistry Council, CISA–2022–0010–0098.

¹⁰³ See, e.g., Comments submitted by American Chemistry Council, CISA–2022–0010–0098; CrowdStrike, CISA–2022–0010–0128.

¹⁰⁴ See, e.g., Comments submitted by BlackBerry; CISA–2022–0010–0036; American Property Casualty Insurance Association, CISA–2022–0010–0064; Computing Technology Industry Association, CISA–2022–0010–0122.

¹⁰⁵ See, e.g., Comments submitted by the Cyber Threat Alliance, CISA–2022–0010–0019; Airlines for America, CISA–2022–0010–0066; Operational Technology Cybersecurity Coalition, CISA–2022–0010–0108; Information Technology-ISAC, CISA–2022–0010–0048; BlackBerry, CISA–2022–0010–0036.

¹⁰⁶ See, e.g., Comments submitted by Exelon Corp., CISA–2022–0010–0043; The Associations: AFPM, AGA, API, APGA, INGAA, LEPA, CISA–2022–0010–0057.

¹⁰⁷ See, e.g., Comment submitted by the Association of Metropolitan Water Agencies, CISA–2022–0010–0088.

¹⁰⁸ See, e.g., Comments submitted by BSA √ The Software Alliance, CISA–2022–0010–0106; SAP, CISA–2022–0010–0114; Information Technology Industry Council, CISA–2022–0010–0097.

¹⁰⁹ See, e.g., Comments submitted by Mandiant, CISA–2022–0010–0120; Accenture, CISA–2022–0010–0077; USTelecom—The Broadband Association, CISA–2022–0010–0067.

¹¹⁰ See, e.g., Comment submitted by Sophos, Inc, CISA–2022–0010–0047 (recommending that information preserved should include at least all logs containing data related to the incident, such as network logs, system logs, and access logs; all correspondence with attackers, including any notes taken during any unrecorded interactions; all identified TTPs and indicators of compromise; all data related to any ransomware payment; and contact information of individuals and entities that provided tactical support in the incident response and investigation process).

¹¹¹ See, e.g., Comments submitted by Sophos, Inc., CISA–2022–0010–0047; SAP, CISA–2022–0010–0114; National Association of Chemical Distributors, CISA–2022–0010–0056.

¹¹² See, e.g., Comments submitted by National Association of Secretaries of State, CISA–2022–0010–0054; OCHIN, CISA–2022–0010–0039; HIMSS Electronic Health Record Association, CISA–2022–0010–0040; Alliance for Automotive Innovation,

Commenters frequently recommended that CISA consult with other Federal departments and agencies with pre-existing regulatory authority in the commenters' particular sectors to avoid duplicative requirements in the CIRCIA regulation. Numerous commenters recommended that, alongside harmonization efforts, CISA should establish a single, national point of contact or process for mandatory cyber incident reporting,¹¹³ suggesting that DHS or CISA serve as the primary or sole entity for receiving and disseminating cyber incident report information.¹¹⁴ Many commenters, noting the language in CIRCIA to this effect, encouraged CISA to implement the reporting exemption for covered entities that submit cyber incident reports with substantially similar information to other Federal departments and agencies, within a substantially similar timeframe.¹¹⁵ A few commenters offered criteria for determining whether a report submitted to another Federal entity constitutes "substantially similar reported information."¹¹⁶ Commenters also offered suggestions on which existing reporting obligations should be considered to include substantially similar information. These suggestions

CISA-2022-0010-0082; Lucid Motors, CISA-2022-0010-0078; Center for Democracy & Technology, CISA-2022-0010-0068.

¹¹³ See, e.g., Comments submitted by Indiana Municipal Power Agency, CISA-2022-0010-0018; HIMSS, CISA-2022-0010-0119; Exelon Corp., CISA-2022-0010-0043; MITRE, CISA-2022-0010-0073; Options Security Corporation, CISA-2022-0010-0160; Airport Council International North America, CISA-2022-0010-0135; Cameron Braatz, CISA-2022-0010-0154.

¹¹⁴ See, e.g., Comments submitted by The Associations, CISA-2022-0010-0057; AFPM, AGA, API, APGA, INGAA, LEPA; Google Cloud, CISA-2022-0010-; Express Association of America, CISA-2022-0010-0038; Workgroup for Electronic Data Interchange, CISA-2022-0010-0041; internet Infrastructure Coalition, CISA-2022-0010-0055; American Council of Life Insurers, CISA-2022-0010-0095; Business Roundtable, CISA-2022-0010-0115.

¹¹⁵ See, e.g., Comments submitted by the American Public Power Association and the Large Public Power Council, CISA-2022-0010-0028; National Rural Electric Cooperative Association, CISA-2022-0010-0025; California Special Districts Association, CISA-2022-0010-0042; Professional Services Council, CISA-2022-0010-0044; American Association of Port Authorities, CISA-2022-0010-0126; Virginia Port Authority, CISA-2022-0010-0052; CHIME, CISA-2022-0010-0035; AHIP, CISA-2022-0010-0091.

¹¹⁶ See, e.g., Comments submitted by Payments Leadership Council, CISA-2022-0010-0031 (recommending CISA consider a report to include substantially similar information if "the material essence of the incident is reflected in the information contained within the report to the other federal entity"); BSA | The Software Alliance, CISA-2022-0010-0106 (recommending that there be a "rebuttable presumption that a report provided by a covered entity to another federal entity is substantially similar").

included the Cyber Incident Notification Requirements for Federally Insured Credit Unions (FICUs), located at 12 CFR 748.1;¹¹⁷ the DFARS incident reporting requirement, located at 48 CFR 252.204-7012;¹¹⁸ Cyber Security Event Notifications for Commercial Nuclear Power Reactors, located at 10 CFR 73.77; TSA Security Directive Pipeline-2021-01 series, Enhancing Pipeline Cybersecurity;¹¹⁹ and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Breach Notification Rule, located at 45 CFR 164.400-414, and corresponding Health Information Technology for Economic and Clinical Health (HITECH) Act Health Breach Notification Rule, located at 16 CFR part 318, which applies to entities not subject to the HIPAA Breach Notification Rule.¹²⁰

xi. Comments on Noncompliance and Enforcement

A small number of commenters offered recommendations related to noncompliance and enforcement of the CIRCIA regulations. These commenters encouraged CISA to keep in mind that covered entities are victims of an incident¹²¹ and recommended that CISA focus on collaboration, not enforcement.¹²² Similarly, a number of commenters recommended that CISA not penalize entities for reporting in good faith under the rule.¹²³ Such possible penalties that commenters recommended CISA avoid included pursuing enforcement under CIRCIA or allowing CIRCIA Reports to be the basis for enforcement actions by other Federal departments and agencies under separate regulations.¹²⁴ One commenter suggested that non-profit, self-incorporated fire and Emergency Management Service departments be excluded from enforcement in the same

¹¹⁷ See, e.g., Comment submitted by NAFCU, CISA-2022-0010-0076.

¹¹⁸ See, e.g., Comments submitted by U.S. Chamber of Commerce, CISA-2022-0010-0075; National Defense ISAC, CISA-2022-0010-0144.

¹¹⁹ See, e.g., Comments submitted by Energy Transfer LP, CISA-2022-0010-0037

¹²⁰ See Comment submitted by Nuclear Energy Institute, CISA-2022-0010-0029; see also comment submitted by Blue Cross Blue Shield Association, CISA-2022-0010-0103.

¹²¹ See, e.g., Comments submitted by the National Technology Security Coalition, CISA-2022-0010-0061; The Associations: BPI, ABA, IIB, SIFMA, CISA-2022-0010-0046.

¹²² See, e.g., Comments submitted by Airlines for America, CISA-2022-0010-0066; Connected Health Initiative, CISA-2022-0010-0130; ACT—The App Association CISA-2022-0010-0129.

¹²³ See, e.g., Comments submitted by the Association of American Railroads, CISA-2022-0010-0117; SolarWinds, CISA-2022-0010-0027; NTCA—The Rural Broadband Association, CISA-2022-0010-0100.

¹²⁴ *Id.*

manner as SLTT Government Entities.¹²⁵

xii. Comments on Treatment and Restrictions on Use of CIRCIA Reports

Numerous commenters provided recommendations on the treatment and restrictions on use of CIRCIA Reports and information therein. One consistent theme throughout the comments on this topic was the notion that CISA should take steps to ensure the confidentiality of the information, including the identity of the victims of reported cyber incidents, included in CIRCIA Reports.¹²⁶ Some of the procedural strategies recommended by commenters to achieve this include having CISA anonymize and aggregate cyber incident report information prior to sharing it with others,¹²⁷ exempting CIRCIA Reports and/or the information contained therein from release under FOIA and similar state laws,¹²⁸ and considering treating CIRCIA Reports as Protected Critical Infrastructure Information, "confidential," or "secret."¹²⁹ Numerous commenters also stressed the need for CISA to protect information submitted in CIRCIA Reports through strong data protection standards, data security practices, and data privacy safeguards.¹³⁰

Commenters also suggested several different limitations on the use of the information contained in CIRCIA Reports. A number of commenters recommended CISA include adequate liability protections in the proposed regulation.¹³¹ Other commenters recommended CISA clarify that reporting does not result in the waiver

¹²⁵ See, e.g., Comment submitted by the International Association of Fire Chiefs, CISA-2022-0010-0081.

¹²⁶ See, e.g., Comments submitted by IBM, CISA-2022-0010-0069; Gideon Rasmussen, CISA-2022-0010-0011; Institute of International Finance, CISA-2022-0010-0060; Powder River Energy Corporation, CISA-2022-0010-0099.

¹²⁷ See, e.g., Comments submitted by Fidelity National Information Services, CISA-2022-0010-0033; UnityPoint Health, CISA-2022-0010-0107; Institute of International Finance, CISA-2022-0010-0060.

¹²⁸ See, e.g., Comments submitted by Edison Electric Institute, CISA-2022-0010-0079; HIMSS, CISA-2022-0010-0119; National Grain and Feed Association, CISA-2022-0010-0104; NAFCU, CISA-2022-0010-0076.

¹²⁹ See, e.g., Comments submitted by NCTA, CISA-2022-0010-0102; SAP, CISA-2022-0010-0114.

¹³⁰ See, e.g., Comments submitted by the Financial Services Sector Coordinating Council, CISA-2022-0010-0094; The Clearing House, CISA-2022-0010-0086; Payments Leadership Council, CISA-2022-0010-0031.

¹³¹ See, e.g., Comments submitted by American Chemistry Council, CISA-2022-0010-0098; SolarWinds, CISA-2022-0010-0027; The Associations: BPI, ABA, IIB, SIFMA, CISA-2022-0010-0046.

of attorney-client privilege, trade secret protections, or other privileges or protections.¹³² A few commenters recommended that information contained in CIRCIA Reports be protected from discovery in civil or criminal actions.¹³³ One commenter recommended that the various protections afforded to CIRCIA Reports still apply even in the event that a CIRCIA Report is compromised (*i.e.*, accessed by an unauthorized individual or made public in an unauthorized manner).¹³⁴

IV. Discussion of Proposed Rule

A. Definitions

Section 226.1 of the proposed rule contains proposed definitions for certain terms used within the rule. These proposed definitions are intended to help clarify the meaning of various terms used throughout the proposed rule and promote consistency in application of the regulatory requirements.

For a number of the terms, CISA proposes using, either verbatim or with minor adjustments, definitions provided in the Definitions sections of CIRCIA, as amended (6 U.S.C. 681). For several other terms where CIRCIA does not include a CIRCIA-specific definition, CISA proposes using, either verbatim or with minor adjustments, definitions provided in the Definitions sections at Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) or at the beginning of Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 650), each as amended, since definitions in those sections also apply to CIRCIA. Proposed definitions that are derived from these legal authorities include: *cloud service provider; cyber incident; Cybersecurity and Infrastructure Security Agency or CISA; cybersecurity threat; Director; information system; managed service provider; ransom payment; ransomware attack; supply chain compromise; and virtual currency.*

Additionally, CISA is proposing definitions for a variety of terms that will have a specific meaning within the proposed regulation. These include *CIRCIA; CIRCIA Agreement; CIRCIA Report; covered cyber incident; Covered Cyber Incident Report; covered entity;*

Joint Covered Cyber Incident and Ransom Payment Report; personal information; Ransom Payment Report; State, Local, Tribal, or Territorial Government entity or SLTT Government entity; substantial cyber incident; and Supplemental Report. The basis for each of these proposed definitions is discussed in their respective subsection below.

i. Covered Entity

Covered entity is a key term in the proposed regulation as, among other things, it is the operative term used to describe the regulated parties responsible for complying with the covered cyber incident and ransom payment reporting and data and records preservation requirements in the proposed CIRCIA regulation. While the statute includes a definition for the term covered entity, the statute explicitly requires CISA to further clarify the meaning of that term through description in the CIRCIA rulemaking. Specifically, the statute defines covered entity to mean “an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 681b(b) of this title.” 6 U.S.C. 681(4). CIRCIA also requires CISA to include a “clear description of the types of entities that constitute covered entities” in the final rule based on various specified factors. 6 U.S.C. 681b(c)(1).

CISA proposes to provide the criteria for covered entities in an Applicability section at § 226.2 of the regulation with a cross-reference to the Applicability section in the Definitions section under the term covered entity. See Section IV.B below and § 226.2 for a detailed discussion of the proposed covered entity criteria and the “clear description of the types of entities that constitute covered entities,” required by 6 U.S.C. 681b(c)(1).

ii. Cyber Incident, Covered Cyber Incident, and Substantial Cyber Incident

1. Cyber Incident

CISA is proposing to include in the regulation a definition of the term cyber incident. The definition of cyber incident is important as it will help bound the types of incidents that trigger reporting requirements for covered entities under the proposed regulation.

CIRCIA states that the term cyber incident “(A) has the meaning given the term ‘incident’ in section 2209; and (B) does not include an occurrence that imminently, but not actually, jeopardizes—(i) information on

information systems; or (ii) information systems.” See 6 U.S.C. 681(5). Section 2209’s definition of “incident” has since been moved to Section 2200 and defines the term “incident” as “an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.” See 6 U.S.C. 650(12).¹³⁵

CISA is proposing to define cyber incident to mean an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually jeopardizes, without lawful authority, an information system. The definition would use the 6 U.S.C. 650 definition verbatim other than striking the “imminently jeopardizes” clause in that definition, as required by 6 U.S.C. 681(5)(B).

2. Covered Cyber Incident

CIRCIA requires CISA to include within the proposed rule a definition for the term covered cyber incident. See 6 U.S.C. 681(3). Because CIRCIA requires covered entities to report only those cyber incidents that qualify as covered cyber incidents to CISA, this definition is essential for triggering the reporting requirement. CISA is proposing to define the term covered cyber incident to mean a substantial cyber incident experienced by a covered entity. CISA also proposes definitions for both substantial cyber incident and covered entity within this NPRM.

Within CIRCIA, Congress defined a covered cyber incident as “a substantial cyber incident experienced by a covered entity that satisfies the definition and

¹³⁵ The definition of “incident” was moved from Section 2209 of the Homeland Security Act (6 U.S.C. 659) to Section 2200 of the Homeland Security Act (6 U.S.C. 650(12)) as part of the consolidation of definitions in Section 7143 (CISA Technical Corrections and Improvements) of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (hereinafter, “CISA Technical Corrections”). Public Law 117–263, Div. G, Title LXXI, § 7143, Dec. 23, 2022. Section (f)(2) of the CISA Technical Corrections includes a rule of construction that provides that “[a]ny reference to a term defined in the Homeland Security Act of 2002 (6 U.S.C. 101 *et seq.*) on the day before the date of enactment of this Act that is defined in section 2200 of that Act pursuant to the amendments made under this Act shall be deemed to be a reference to that term as defined in section 2200 of the Homeland Security Act of 2002, as added by this Act.” Pursuant to this rule of construction, the cross-reference in CIRCIA’s definition of “cyber incident” to the definition of “incident” in Section 2209 of the Homeland Security Act (6 U.S.C. 659) is deemed a reference to the definition of “incident” in Section 2200 of the Homeland Security Act (6 U.S.C. 650).

¹³² See, *e.g.*, Comments submitted by CrowdStrike, CISA–2022–0010–0128; U.S. Chamber of Commerce, CISA–2022–0010–0075; Connected Health Initiative, CISA–2022–0010–0130.

¹³³ See, *e.g.*, Comments submitted by Connected Health Initiative, CISA–2022–0010–0130; ACT | The App Association, CISA–2022–0010–0129.

¹³⁴ See Comment submitted by submitted by Health-ISAC and the Healthcare and Public Health Sector Coordinating Council Cybersecurity Working Group, CISA–2022–0010–0123.

criteria established by the Director in the final rule issued pursuant to section 681b(b) of this title.” See 6 U.S.C. 681(3). CISA believes that defining a covered cyber incident to include all substantial cyber incidents experienced by a covered entity rather than some subset thereof is both consistent with the statutory definition of covered cyber incident and is the least complicated approach to defining covered cyber incidents.

Under this approach, a covered entity simply needs to determine if a cyber incident is a substantial cyber incident for it to be reported, rather than having to perform an additional analysis to determine if a substantial cyber incident meets some narrower criteria for a covered cyber incident. As the term substantial cyber incident is not used in CIRCIA other than to help define a covered cyber incident, CISA does not see any benefit to having one set of requirements for what constitutes a substantial cyber incident and a separate set of requirements for which substantial cyber incidents experienced by a covered entity qualify as covered cyber incidents.

3. Substantial Cyber Incident

CISA is proposing to include within the rule a definition for the term substantial cyber incident. Given CISA’s proposal to define a covered cyber incident as a substantial cyber incident experienced by a covered entity, the term substantial cyber incident is essential to the CIRCIA regulation as it identifies the types of incidents that, when experienced by a covered entity, must be reported to CISA.

While CIRCIA does not define the term substantial cyber incident, it provides minimum requirements for the types of substantial cyber incidents that qualify as covered cyber incidents. See 6 U.S.C. 681b(c)(2)(A). Consistent with these minimum requirements, CISA proposes the term substantial cyber incident to mean a cyber incident that leads to any of the following: (a) a substantial loss of confidentiality, integrity, or availability of a covered entity’s information system or network; (b) a serious impact on the safety and resiliency of a covered entity’s operational systems and processes; (c) a disruption of a covered entity’s ability to engage in business or industrial operations, or deliver goods or services; or (d) unauthorized access to a covered entity’s information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting

provider, or a supply chain compromise. CISA is further proposing that a substantial cyber incident resulting in one of the listed impacts include any cyber incident regardless of cause, including, but not limited to, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability. Finally, CISA is proposing the term substantial cyber incident does not include (a) any lawfully authorized activity of a United States Government entity or SLTT Government entity, including activities undertaken pursuant to a warrant or other judicial process; (b) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; or (c) the threat of disruption as extortion, as described in 6 U.S.C. 650(22).¹³⁶

In developing this proposed definition, CISA examined how other Federal departments and agencies that regulate cyber incident reporting define similar terminology for their reporting regimes, reviewed the Model Definition for a Reportable Cyber Incident proposed by the Secretary of Homeland Security in the CIRC-informed DHS Report to Congress (the “CIRC Model Definition”), and considered the many comments received on this topic from stakeholders both at CIRCIA listening sessions and in written comments submitted in response to the CIRCIA RFI. CISA considered those various perspectives and approaches both within the constraints explicitly imposed by CIRCIA and in light of the purposes for which CISA believes CIRCIA was created as described in Section III.C in this document.

The proposed definition contains the following elements: (1) a set of four threshold impacts which, if one or more occur as the result of a cyber incident, would qualify that cyber incident as a substantial cyber incident; (2) an explicit acknowledgment that substantial cyber incidents can be

¹³⁶ The definition of ransomware attack contained in Section 2240(14)(A) was originally codified in 6 U.S.C. 681(14) but was moved from 6 U.S.C. 681(14) to 6 U.S.C. 650(22) as part of the consolidation of definitions in the CISA Technical Corrections, *supra* note 135. The CISA Technical Corrections, however, did not update this cross-reference in CIRCIA. Nevertheless, pursuant to the rule of construction in Section (f)(2) of the CISA Technical Corrections, the cross reference in 6 U.S.C. 681b(c)(2)(C)(ii) to part of the definition of ransomware attack in 6 U.S.C. 681(14) is deemed a reference to the definition of ransomware attack now in 6 U.S.C. 650 (Section 2200 of the Homeland Security Act).

caused through compromises of third-party service providers or supply chains, as well as various techniques and methods; and (3) three separate types of incidents that, even if they were to meet the other criteria contained within the substantial cyber incident definition, would be excluded from treatment as a substantial cyber incident. Each of these elements is addressed in turn below.

a. Minimum Requirements for a Cyber Incident To Be a Substantial Cyber Incident

While Congress did not define the term substantial cyber incident in CIRCIA, Congress did include minimum requirements for the types of substantial cyber incidents that constitute covered cyber incidents. See 6 U.S.C. 681b(c)(2)(A).¹³⁷ Because CISA is proposing that a covered cyber incident mean any substantial cyber incident experienced by a covered entity (see Section IV.A.ii.2 in this document), CISA interprets the minimum requirements enumerated in 6 U.S.C. 681b(c)(2)(A) as the minimum requirements an incident must meet to be considered a substantial cyber incident (as opposed to a subset of substantial cyber incidents that constitute covered cyber incidents). Thus, while CISA has discretion to raise the threshold required for something to be a substantial cyber incident, resulting in a reduction of the number of incidents that would qualify as substantial, CISA may not lower the threshold below the requirements enumerated in 6 U.S.C. 681b(c)(2)(A).

CISA believes that the minimum requirements enumerated in 6 U.S.C. 681b(c)(2)(A) create a sufficiently high threshold to prevent overreporting by making it clear that routine or minor cyber incidents do not need to be reported. Accordingly, CISA is proposing to use those requirements as the basis for the first part of the definition of substantial cyber incident,

¹³⁷ 6 U.S.C. 681b(c)(2)(A) states that the types of substantial cyber incidents that constitute covered cyber incidents must, “at a minimum, require the occurrence of (i) a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes; (ii) a disruption of business or industrial operations, including due to a denial-of-service attack, ransomware attack, or exploitation of a zero day vulnerability, against (I) an information system or network; or (II) an operational technology system or process; or (iii) unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise.”

with minor modifications for clarity and for greater consistency with the CIRC Model Definition of a reportable cyber incident. Ultimately, CISA is proposing four types of impacts that, if experienced by a covered entity as a result of a cyber incident, would result in the incident being classified as a substantial cyber incident and therefore reportable under the CIRCIA regulation. Each of these impact types is described in its own prong of the substantial cyber incident definition.

i. Impact 1: Substantial Loss of Confidentiality, Integrity, or Availability

Under the first proposed threshold impact, a cyber incident would be considered a substantial cyber incident if it resulted in a substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network. See § 226.1 of the proposed regulation. This impact reflects the substantive criteria contained in the first part of 6 U.S.C. 681b(c)(2)(A)(i), which states "a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of such information system or network." Although this prong does not explicitly mention operational technology (OT), CISA is using the term "information system," (which, per the proposed definition, as described in Section IV.A.iv.7 in this document, includes OT) in this threshold and proposes to interpret this aspect of the regulation to also specifically cover cyber incidents that lead to substantial loss of confidentiality, integrity, or availability of a covered entity's OT.

The concepts of confidentiality, integrity, and availability (CIA), often referred to as the "CIA triad," represent the three pillars of information security.¹³⁸ "Confidentiality" refers to "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."¹³⁹ "Integrity" refers to "guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity."¹⁴⁰ "Availability" refers to "ensuring timely and reliable access to and use of information."¹⁴¹

The loss of CIA of an information system, including OT, or network can occur in many ways. For example, if an

unauthorized individual steals credentials or uses a brute force attack to gain access to a system, they have caused a loss of the confidentiality of a system. If that unauthorized individual uses that access to modify or destroy any information on the system, they have caused a loss of the integrity of the system and potentially a loss of the availability of the information contained therein. A denial-of-service attack that renders a system or network inaccessible is another example of an incident that leads to a loss of the availability of the system or network. These are just some of the many types of incidents that can lead to a loss of CIA and would be reportable if the impacts are "substantial."

Whether a loss of CIA constitutes a "substantial" loss will likely depend on a variety of factors, such as the type, volume, impact, and duration of the loss. One example of a cyber incident that typically would meet the "substantial" threshold for this impact type is a distributed denial-of-service attack that renders a covered entity's service unavailable to customers for an extended period of time. Similarly, a ransomware attack or other attack that encrypts one of a covered entity's core business or information systems substantially impacting the confidentiality, availability, or integrity of the entity's data or services likely also would meet the threshold of a substantial cyber incident under this first impact type and would need to be reported under the CIRCIA regulation. Persistent access to information systems by an unauthorized third party would typically be considered a substantial loss of confidentiality. By contrast, even time-limited access to certain high-value information systems, such as access to privileged credentials or to a domain controller, could also be considered a substantial loss of confidentiality. A large-scale data breach or otherwise meaningful exfiltration of data typically would also be considered a substantial cyber incident as it would reflect a substantial loss of the confidentiality of an information system. A theft of data that may or may not itself meet the "substantial" impact threshold by nature of the data theft alone (based on the type or volume of data stolen) could become a substantial cyber incident if the theft is followed by a data leak or a credible threat to leak data.

Conversely, CISA would not expect a denial-of-service attack or other incident that results in a covered entity's public-facing website being unavailable for a few minutes to typically rise to the level

of a substantial cyber incident under this impact.¹⁴²

ii. Impact 2: Serious Impact on Safety and Resiliency of Operational Systems and Processes

The second impact type of the proposed substantial cyber incident definition would require a covered entity to report a cyber incident that results in a serious impact on the safety and resiliency of a covered entity's operational systems and processes. This impact reflects the threshold enumerated in the second part of 6 U.S.C. 681b(c)(2)(A)(i), which states "a cyber incident that leads to . . . a serious impact on the safety and resiliency of operational systems and processes." Safety is a commonly understood term, which NIST defines as "[f]reedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment."¹⁴³ NIST defines resilience as "[t]he ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption," and operational resilience as "[t]he ability of systems to resist, absorb, and recover from, or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of the ability to perform mission-related functions."¹⁴⁴

Similar to the interpretation of the word "substantial" in the first impact type, whether an impact on the safety and resiliency of an operational system or process is "serious" will likely depend on a variety of factors, such as the safety or security hazards associated with the system or process, and the scale and duration of the impact. For example, a cyber incident that noticeably increases the potential for a release of a hazardous material used in chemical manufacturing or water purification likely would meet this

¹⁴² The examples provided in this paragraph and elsewhere in this section of what typically might or might not be considered a substantial cyber incident are simply a few sample scenarios meant to provide context around this discussion. The examples are not meant as an exhaustive or definitive list of what is and is not a substantial cyber incident. Whether something is or is not a substantial cyber incident is fact-dependent and must be assessed on a case-by-case basis. For example, while, as noted, an incident resulting in a brief unavailability of a public-facing website would typically not qualify as a substantial loss of availability, such an incident may be significant for a covered entity whose public-facing website is a core part of its service offering (such as a webmail provider).

¹⁴³ NIST, *Developing Cyber-Resilient Systems*, NIST Special Publication 800–160 Vol. 2 Rev. 1, at 67 (Dec. 2021), available at <https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final>.

¹⁴⁴ *Id.* at 65–66.

¹³⁸ See, e.g., NIST, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, NIST Special Publication 1800–25 Vol. A at 1 (Dec. 2020), available at <https://csrc.nist.gov/pubs/sp/1800/25/final>.

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

definition. Similarly, a cyber incident that compromised or disrupted a BES cyber system that performs one or more reliability tasks would also likely meet this prong of the substantial cyber incident definition. Further, a cyber incident that disrupts the ability of a communications service provider to transmit or deliver emergency alerts or 911 calls, or results in the transmission of false emergency alerts or 911 calls, would meet this definition. While CISA anticipates that the types of incidents that will actually lead to a serious impact to the safety and resilience of operational systems and processes may frequently involve OT, CISA does not interpret “operational systems and processes” to be a reference to OT. Congress used the specific phrase “operational technology” elsewhere in CIRCIA—including in the immediate next provision—and therefore certainly could have used it in this provision if that was the intent. Compare 6 U.S.C. 681b(c)(2)(A)(i) with 6 U.S.C. 681b(c)(2)(A)(ii)(II). Accordingly, CISA interprets this prong broadly as not being limited to only incidents impacting OT, and covered entities should report incidents that are covered cyber incidents under this prong of the definition even if the impacts that meet the threshold are not to OT.

iii. Impact 3: Disruption of Ability To Engage in Business or Industrial Operations

The third impact of the proposed substantial cyber incident definition would require a covered entity to report an incident that results in a disruption of a covered entity’s ability to engage in business or industrial operations, or deliver goods or services. This prong reflects criteria enumerated by Congress in both 6 U.S.C. 681b(c)(2)(A)(ii) and (iii), which provides that one type of incident that could qualify as a substantial cyber incident that constitutes a covered cyber incident is a cyber incident that causes a disruption of business or industrial operations, including due to a denial-of-service attack, ransomware attack, or exploitation of a zero-day vulnerability, against (I) an information system or network; or (II) an operational technology system or process; or unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a CSP, managed service provider, or other third-party data hosting provider or by a supply chain compromise.

In drafting this prong, CISA has added two clauses to the statutory criteria relating to an entity’s ability to engage

in business operations or deliver goods or services. CISA proposes adding these clauses to this prong of the substantial cyber incident definition to clarify CISA’s understanding of the statutory language. CISA understands that a disruption of business operations includes a disruption to an entity’s ability to engage in business operations and the ability to deliver goods or services. CISA considers this language to be a clarification of the statutory language, and not an expansion.

NIST defines a disruption as “[a]n unplanned event that causes a . . . system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).”¹⁴⁵ As opposed to the statutory source for the first two prongs of this definition, the portion of CIRCIA from which this prong is drawn does not contain a qualifier such as “substantial” or “serious.” Nevertheless, because this prong is part of the threshold for a “substantial” cyber incident, CISA believes it is appropriate to read into the prong some level of significance. Like the previous prongs, whether a disruption rises to the level of reportability may depend on a variety of factors and circumstances, such as the scope of the disruption and what was disrupted. A relatively minor disruption to a critical system or network could rise to a high level of substantiality, while a significant disruption to a non-critical system or network might not. Generally speaking, incidents that result in minimal or insignificant disruptions are unlikely to rise to the level of a substantial cyber incident reportable under this prong; however, the specific circumstances of the disruption should be taken into consideration.

While 6 U.S.C. 681b(c)(2)(A)(ii) provides that this category includes disruptions of business or industrial operations “due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability,” CISA is not proposing to include this language in this third prong, as CISA reads this language as being illustrative of the types of incidents that might lead to a disruption of business or industrial operations, rather than a limitation on the types of incidents that can be reportable under this prong. To that end, examples of cyber incidents that would meet this prong include the exploitation of a zero-

day vulnerability resulting in the extended downtime of a covered entity’s information system or network, a ransomware attack that locks a covered entity out of its industrial control system, or a distributed denial-of-service attack that prevents customers from accessing their accounts with a covered entity for an extended period of time. Another example would be where a critical access hospital is unable to operate due to a ransomware attack on a third-party medical records software company on whom the critical access hospital relies; the critical access hospital, and perhaps the medical records software company as well if it also is a covered entity, would need to report the incident. Cyber incidents that result in minor disruptions, such as short-term unavailability of a business system or a temporary need to reroute network traffic, typically would not be considered substantial under this prong.

iv. Impact 4: Unauthorized Access Facilitated Through or Caused by a: (1) Compromise of a CSP, Managed Service Provider, or Other Third-Party Data Hosting Provider, or (2) Supply Chain Compromise

The fourth prong of the proposed substantial cyber incident definition would require a covered entity to report an incident that results in unauthorized access to a covered entity’s information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a compromise of a CSP, managed service provider, other third-party data hosting provider, or by a supply chain compromise. This prong reflects criteria enumerated in 6 U.S.C. 681b(c)(2)(A)(iii).

NIST defines unauthorized access as occurring when an individual “gains logical or physical access without permission to a network, system, application, data, or other resource.”¹⁴⁶ Unauthorized access causes actual jeopardy to information systems and the information therein by compromising the first pillar of the CIA triad—confidentiality—and by providing an adversary with a launching off point for additional penetration of a system or network. Much like the third prong, the source language in CIRCIA does not contain any qualifier such as “substantial” or “serious.” However, unlike that prong, CISA understands the absence of a qualifier here to be a reflection of the seriousness of

¹⁴⁵ NIST, *Contingency Planning Guide for Federal Information Systems*, NIST Special Publication 800–34 Rev. 1, Appendix G, (May 2010), available at <https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final>.

¹⁴⁶ NIST, *Guide to Industrial Control Systems Security*, NIST Special Publication 800–82 Rev. 3, at 168 (Sept. 2023), available at <https://csrc.nist.gov/pubs/sp/800/82/r3/final>.

unauthorized access through a third party (such as a managed service provider or CSP) or a supply chain compromise. Such cyber incidents uniquely have the ability to cause significant or substantial nation-level impacts, even if the impacts at many of the individual covered entities are relatively minor. The legislative intent makes clear that supply chain compromises such as the “SUNBURST” malware that compromised legitimate updates of customers using the SolarWinds Orion product, and third-party incidents like the compromise of the managed service provider Kaseya, were major drivers of the passage of CIRCIA.¹⁴⁷ CISA therefore understands that this prong reflects a recognition that CISA needs visibility into the breadth of a third-party incident or supply chain compromise to adequately meet its obligations under CIRCIA.

Examples of cyber incidents that CISA typically would consider meeting this prong include a detected, unauthorized intrusion into an information system or the exfiltration of information as a result of a supply chain compromise (see Section IV.A.iv.13 for further discussion on the meaning of supply chain compromise). Similarly, unauthorized access that was achieved through exploitation of a vulnerability in the cloud services provided to a covered entity by a CSP or by leveraging access to a covered entity’s system through a managed service provider would meet this prong. Conversely, because the statute requires the unauthorized access to have been facilitated through or caused by a compromise of a third-party service provider or supply chain compromise, unauthorized access that results from a vulnerability within

proprietary code developed by the covered entity or a gap in the covered entity’s access control procedures that allows an unauthorized employee administrative access to the system would not constitute a substantial cyber incident under this prong (though could still qualify as a substantial cyber incident under one of the first three prongs if it resulted in the requisite impact levels).

b. Guidance for Assessing Whether an Impact Threshold Is Met

When evaluating whether a cyber incident meets one of the four proposed impact thresholds that would qualify it as a substantial cyber incident, a covered entity should keep in mind several principles. First, an incident needs to meet only one of the four prongs, not all four of the prongs, for it to be a substantial cyber incident. CISA believes Congress’s use of the word “or” in 6 U.S.C. 681b(c)(2)(A) was intentional and was meant to confer the fact that for an incident to be a substantial cyber incident that meets the threshold of a covered cyber incident it only had to meet one of the enumerated criteria, not all the enumerated criteria. CISA’s proposed definition for substantial cyber incident follows this example, using “or” intentionally to indicate that if an incident meets any of the enumerated criteria within the definition it is a substantial cyber incident. This approach is also consistent with the CIRC Model Definition, with which, for the reasons discussed below, CISA attempted to align to the extent practicable.

Second, for an incident to qualify as a substantial cyber incident, CISA interprets CIRCIA to require the incident to actually result in one or more of the impacts described above. A number of other cyber incident reporting regulations do not require actual impacts for an incident to have to be reported; rather, some require reporting if an incident results in imminent or potential harm, or identification of a vulnerability. While good policy rationales exist for both approaches in various contexts, CISA believes the phrase “require the occurrence of” in 6 U.S.C. 681b(c)(2)(A) limits reportable incidents under CIRCIA to those that have actually resulted in at least one of the impacts described in that section of CIRCIA. Likewise, CIRCIA’s definition of cyber incident (of which substantial cyber incidents are a subset) specifically omits occurrences imminently, but not actually, jeopardizing information systems or information on information systems. 6 U.S.C. 681(5). Consequently,

if a cyber incident jeopardizes an entity or puts the entity at imminent risk of threshold impacts but does not actually result in any of the impacts included in the proposed definition, the cyber incident does not meet the definition of a substantial cyber incident. Similarly, if malicious cyber activity is thwarted by a firewall or other defensive or mitigative measure before causing the requisite level of impact, it would not meet the proposed definition of a substantial cyber incident and would not have to be reported. Consequently, blocked phishing attempts, failed attempts to gain access to systems, credentials reported missing but that have not been used to access the system and have since been rendered inactive, and routine scanning that presents no evidence of penetration are examples of events or incidents that typically would not be considered substantial cyber incidents. To both convey this intention and to more closely align with the language used in the CIRC Model Definition, CISA is proposing “a cyber incident that leads to” as the introductory language before the enumerated threshold prongs. CISA believes the phrase “leads to” satisfactorily conveys that a covered entity must have experienced one of the enumerated impacts for an incident to be considered a substantial cyber incident.

Third, the type of TTP used by an adversary to perpetrate the cyber incident and cause the requisite level of impact is typically irrelevant to the determination of whether an incident is a substantial cyber incident.¹⁴⁸ CISA believes that the specific attack vector or TTP used to perpetrate the incident (e.g., malware, denial-of-service, spoofing, phishing) should not be relevant to determining if an incident is a substantial cyber incident if one of the impact threshold prongs are met. One of the primary purposes of the CIRCIA regulation is to allow CISA the ability to identify TTPs being used by adversaries to cause cyber incidents. Limiting reporting to a specific list of TTPs that CISA currently is aware of would inhibit CISA’s ability to fully understand the dynamic cyberthreat landscape as it evolves over time or be able to warn infrastructure owners and

¹⁴⁷ See, e.g., *CHS Fact Sheet*, *supra* note 16, (referencing the SolarWinds supply chain compromise); Comm. on Homeland Security and Governmental Affairs, Staff Report: America’s Data Held Hostage: Case Studies in Ransomware Attacks on American Companies, 25–27 (Mar. 2022) (discussing the Kaseya ransomware attacks), available at <https://www.hsgac.senate.gov/library/files/americas-data-held-hostage-case-studies-in-ransomware-attacks-on-american-companies/>; Business Meeting, Homeland Security and Governmental Affairs Committee, Opening Remarks by Ranking Member Rob Portman (Oct. 6, 2021), (citing SolarWinds as an example of an event that shows why greater transparency of these types of events through cyber incident reporting to CISA is needed), available at <https://www.hsgac.senate.gov/hearings/10-06-2021-business-meeting/>; *Stakeholder Perspectives Hearing*, *supra* note 17, at 55 (Statement of Rep. James Langevin) (“The SolarWinds breach has brought new attention to the issue of incident reporting, and for good reason.”); 168 Cong. Rec. S1149 (daily ed. Mar. 14, 2022) (statement of Sen. Mark Warner) (“The SolarWinds breach demonstrated how broad the ripple effects of these attacks can be, affecting hundreds or even thousands of entities connected to the initial target.”).

¹⁴⁸ The primary exception is the fourth prong, which is limited to instances where unauthorized access was facilitated through or caused by a compromise of a CSP, managed service provider, or another third-party data hosting provider, or by a supply chain compromise. However, even within this vector-specific prong, the specific TTPs used by the threat actor to compromise a third-party provider or the supply chain is not relevant to whether the incident is reportable.

operators of novel or reemerging TTPs. (See further discussion in Section IV.A.ii.3.f of this document describing why CISA is proposing not to use the sophistication or novelty of the tactics used to narrow the definition of substantial cyber incidents.) This is also consistent with CIRCIA's statutory language, which references certain types of TTPs, such as denial-of-service attacks or exploitation of a zero-day vulnerability, as only examples, rather than a limitation on reportable covered cyber incidents. See 6 U.S.C. 681b(c)(2)(A)(ii).

Fourth, for similar reasons, CISA has elected not to limit the definition of substantial cyber incident to impacts to specific types of systems, networks, or technologies. A number of commenters suggested that CISA should only require reporting of incidents that impact critical systems. CISA is proposing that under CIRCIA, if a cyber incident impacting a system, network, or technology that an entity may not believe is critical nonetheless results in actual impacts that meet the level of one or more of the threshold impact prongs, then the incident should be reported to CISA. In addition to helping ensure CISA receives reports on substantial cyber incidents even if they were perpetrated against a system, network, or technology deemed non-critical by the impacted covered entity, this approach also has the benefit of alleviating the need for a covered entity to proactively determine which systems, networks, or technologies it believes are "critical" and instead focus solely on the actual impacts of an incident as the primary determining factor as to whether a cyber incident is a reportable substantial cyber incident. For similar reasons, CISA is proposing to include, but not specifically distinguish, cyber incidents with impacts to OT. While it may be the case that cyber incidents affecting OT are more likely to meet the impact thresholds in the definition of substantial cyber incident, CISA did not want to artificially scope out cyber incidents that primarily impact business systems but nevertheless result in many of the same type of impacts that could result from a cyber incident affecting OT.

Fifth, CISA is aware that in some cases, a covered entity will not know for certain the cause of the incident within the first few days following the occurrence of the incident. As is discussed in greater detail in Section IV.E.iv on the timing of submission of CIRCIA Reports, a covered entity does not need to know the cause of the incident with certainty for it to be a reportable substantial cyber incident.

For incidents where the covered entity has not yet been able to confirm the cause of the incident, the covered entity must report the incident if it has a "reasonable belief" that a covered cyber incident occurred. If an incident meets any of the impact-based criteria, it would be reportable if the covered entity has a "reasonable belief" that the threshold impacts occurred as a result of activity without lawful authority, even if the specific cause is not confirmed. For the fourth prong, a reasonable belief that unauthorized access was caused by a third-party provider or a supply chain compromise would be sufficient to trigger a reporting obligation, even if the cause of the cyber incident was not yet confirmed. As discussed in Section III.C.ii on the purposes of the regulation, timely reporting is of the essence for CISA to be able to quickly analyze incident reports, identify trends, and provide early warnings to other entities before they can become victims. Accordingly, CISA believes its ability to achieve the regulatory purposes of CIRCIA would be greatly undermined if covered entities were allowed to delay reporting until an incident has been confirmed to have been perpetrated without lawful authority. Therefore, an incident whose cause is undetermined, but for which the covered entity has a reasonable belief that the incident may have been perpetrated without lawful authority, must be reported if the incident otherwise meets the reporting criteria. If, however, the covered entity knows with certainty the cause of the incident, then the covered entity only needs to report the incident if the incident was perpetrated without lawful authority.

Finally, CISA expects a covered entity to exercise reasonable judgment in determining whether it has experienced a cyber incident that meets one of the substantiality thresholds. If a covered entity is unsure as to whether a cyber incident meets a particular threshold, CISA encourages the entity to either proactively report the incident or reach out to CISA to discuss whether the incident needs to be reported.

c. Reportability of Cyber Incidents Regardless of Cause

As noted in Section IV.A.ii.3.a.iv of this document, the CIRCIA statute limits which cyber incidents only involving unauthorized access can be considered a substantial cyber incident. Specifically, the statute states that to be considered a substantial cyber incident based on unauthorized access alone (without any of the impacts listed in the first three prongs, such as where the unauthorized access does not result in

a "substantial" loss of confidentiality, integrity, or availability under the first prong), a cyber incident must be facilitated through or caused by a compromise of a CSP, managed service provider, another third-party data hosting provider, or by a supply chain compromise. See 6 U.S.C. 681b(c)(2)(A)(iii). Cyber incidents resulting in impacts other than unauthorized access and described in the first three impact prongs are not limited by the source or cause in the same manner. Similarly, as noted in Section IV.A.ii.3.a.iii of this document, CISA does not view the language in 6 U.S.C. 681b(c)(2)(A)(ii) regarding denial-of-service attacks, ransomware attacks, or exploitation of a zero-day vulnerability as suggesting a limitation on the vector or type of incidents in the third prong, or to suggest that denial-of-service attacks, ransomware attacks, or exploitation of a zero-day vulnerability that leads to the impacts described in the first two prongs would not be reportable if the impact thresholds are otherwise met. To ensure it is clear that cyber incidents resulting in threshold impacts other than unauthorized access should be reported regardless of cause or vector, including whether they were or were not facilitated through or caused by a compromise of a third-party service provider or supply chain compromise, denial-of-service attack, ransomware attack, or exploitation of a zero-day vulnerability, CISA is proposing to include in the definition of substantial cyber incident explicit language to that effect. Specifically, CISA is proposing to include in the definition of substantial cyber incident the statement that a substantial cyber incident resulting in any of the threshold impacts identified in the first three prongs includes any cyber incident regardless of cause. See proposed § 226.1. As indicated in the proposed regulatory text, CISA interprets the phrase "regardless of cause" to include, but not be limited to, incidents caused by a compromise of a CSP, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability.

In today's complex cyber environment, entities frequently rely on third parties for various IT-related services, such as hosting, administering, managing, or securing networks, systems, applications, infrastructure, and digital information. Depending on what services are being provided, these third-party service providers—be they CSPs, managed service providers, or other third-party data hosting

providers—via the systems and networks they manage, may provide an additional avenue through which nefarious individuals can seek to impact a service provider's customer's information systems or the information contained therein, which may also impact a covered entity. Similarly, adversaries may seek to impact covered entities by exploiting elements of the supply chain that a covered entity may rely upon.

This part of the substantial cyber incident definition is intended, in part, to ensure that a covered entity reports cyber incidents experienced by the covered entity that rise to the level of substantiality that warrants reporting even if the cyber incident in question was caused by a compromise of a product or service managed by someone other than the covered entity. This clause is important to prevent the creation of a "blind spot" where the covered entity experiences a substantial cyber incident but escapes required reporting based on the manner in which the incident was initiated or perpetrated. Congress recognized the importance of this approach, and explicitly authorized it in CIRCIA for incidents that resulted in "unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise." 6 U.S.C. 681b(c)(2)(A)(iii).

CISA believes the policy rationale for applying this provision to incidents resulting in unauthorized access or disruption of business or industrial operations (the third and fourth threshold prongs) applies equally to incidents resulting in a substantial loss of CIA, or a serious impact on the safety and resiliency of operational systems and processes (the first and second prongs). Accordingly, CISA proposes including this clause as a full part of the substantial cyber incident definition, so that it applies to cyber incidents that result in impacts meeting any of the four impact threshold prongs.

While a covered entity must report qualifying incidents that are the result of a compromise of a CSP, managed service provider, or other third-party data hosting provider, or by a supply chain compromise, it is important to note that this imposes reporting requirements solely on the covered entity that the incident impacts at a threshold level. Accordingly, a CSP, managed service provider, or other third-party service provider is not obligated, by virtue of this provision, to

report an incident that causes threshold level impacts to one of its customers even if the impacts are the result of a compromise of the third-party's services, network, software, etc. A third-party service provider only needs to report a cyber incident if (a) the third-party service provider independently meets the definition of covered entity, and (b) the third-party service provider itself experiences impacts that rise to the level of a substantial cyber incident. Note, however, a covered entity third-party provider could experience a reportable substantial cyber incident without the third-party service provider experiencing direct impacts from a cyber incident that exploits or compromises their information networks or systems. This would be the case where a cyber incident facilitated through or caused by a compromise of the third-party service provider meeting the definition of a covered entity caused enough impacts to one or more of the provider's customers that the cumulative effect of the incident resulted in a substantial disruption of the third-party service provider's business operations.

This part of the proposed substantial cyber incident definition is also intended to emphasize that the first three prongs of the definition of substantial cyber incident are also TTP, incident type, and vector agnostic. While denial-of-service attack, ransomware attack, and exploitation of a zero-day vulnerability are specifically listed in this part of the definition in light of their inclusion in 6 U.S.C. 681b(c)(2)(A)(ii), their inclusion in the statute and this part of the definition are as examples only. Any cyber incident experienced by a covered entity, regardless of cause, that meets the impact thresholds in the first three prongs of the definition of substantial cyber incident would be considered a substantial cyber incident. This includes, for example, exploitation of a previously known vulnerability, and not just exploitation of a zero-day vulnerability. For further examples of incidents that typically would and would not be considered a substantial cyber incident, see Section IV.A.ii.3.e of this document.

d. Exclusions

In 6 U.S.C. 681b(c)(2)(C), Congress identified two types of events that CISA must exclude from the types of incidents that constitute covered cyber incidents. Specifically, Congress stated that CISA was to "exclude (i) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or

operator of the information system; and (ii) the threat of disruption as extortion, as described in section 2240(14)(A)." 6 U.S.C. 681b(c)(2)(C). In addition, CISA is proposing excluding any lawfully authorized U.S. Government or SLTT Government entity activity including activities undertaken pursuant to a warrant or other judicial process.

CISA is proposing to incorporate these exclusions into the definition of substantial cyber incident by proposing a statement reiterating these exclusions at the end of the definition itself. The statement added to the proposed definition of substantial cyber incident is taken almost verbatim from the CIRC Model Definition which itself includes both of the exclusions contained in 6 U.S.C. 681b(c)(2)(C). Additional information on each of the prongs of this exclusory statement are contained in the following three subsections.

i. Lawfully Authorized Activities of a United States Government Entity or SLTT Government Entity

CISA proposes excluding from the definition of substantial cyber incident any lawfully authorized United States Government entity or SLTT Government entity activity, including activities undertaken pursuant to a warrant or other judicial process. This exception, which is similar to an exception contained in the CIRC Model Definition, is intended to except from reporting any incident that occurs as the result of a lawful activity of a Federal or SLTT law enforcement agency, Federal intelligence agency, or other Federal or SLTT Government entity. This exception does not, however, allow a covered entity to delay or forgo reporting a covered cyber incident to CISA because it has reported a covered cyber incident to, or is otherwise working with, law enforcement. It simply says that a lawful activity conducted by a Federal or SLTT governmental entity, such as a search or seizure conducted pursuant to a warrant, is not itself a substantial cyber incident.

CISA believes this exception is warranted as reports on lawful Federal or SLTT government activity would in no meaningful way further the articulated purposes of the regulation, such as analyzing adversary TTPs and enabling a better understanding of the current cyber threat environment. This exception provides further clarity on the scope of cyber incident, which is defined as an occurrence "without lawful authority." Moreover, failure to exclude such incidents from required reporting could negatively impact a covered entity's willingness to work

with Federal or SLTT law enforcement, intelligence, or other government agencies if such cooperation could result in new regulatory reporting obligations.

ii. Incidents Perpetrated in Good Faith by an Entity in Response to a Specific Request by the Owner or Operator of the Information System

Section 681b(c)(2)(C)(i) of title 6, United States Code, states that the description of the types of substantial cyber incidents that constitute covered cyber incidents shall exclude “any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system.” CISA is proposing incorporating this exclusion verbatim into the proposed definition of substantial cyber incident.

There are a variety of situations in which a cyber incident could occur at a covered entity as the result of an entity acting in good faith to a request of the owner or operator of the information system through which the cyber incident was perpetrated. One example of this would be if a third-party service provider acting within the parameters of a contract with the covered entity unintentionally misconfigures one of the covered entity’s devices leading to a service outage. Another example would be a properly authorized penetration test that inadvertently results in a cyber incident with actual impacts. Congress intended that such incidents, when the result of good faith actions conducted pursuant to a specific request by the owner or operator of the information system at issue, be excluded from the CIRCIA reporting requirements.

In addition to the examples provided above, CISA interprets this exclusion to also exclude from reporting cyber incidents that result from security research testing conducted by security researchers who have been authorized by the covered entity or the owner or operator of the impacted information system to attempt to compromise the system, such as in accordance with a vulnerability disclosure policy or bug bounty programs published by the owner or operator. However, because the exception only applies to “cyber incident[s] perpetrated in good faith . . . in response to a specific request by” the information system owner or operator, this exception would only apply to this type of research where the bug bounty program, vulnerability disclosure policy, or other form of authorization preceded the discovery of the incident. That said, CISA anticipates that this example would occur rarely, as

good faith security research should generally stop at the point the vulnerability can be demonstrated and should not typically engage in activity that would result in a covered cyber incident.¹⁴⁹

Regarding this exclusion, the request that causes the incident need not necessarily come from the impacted covered entity itself, but rather from the owner or operator of the information system at issue. While the owner or operator of the information system through which the incident was caused will often be the covered entity, that may not always be the case. For example, in some situations involving a CSP or managed service provider, the service provider may duly authorize a penetration test on its own systems or software. If such testing inadvertently resulted in a cyber incident at the service provider, it could have downstream effects on one or more of the service provider’s customers (such as by taking out of operation a key cloud-based software that the customers rely upon for core operations). Such downstream effects could themselves constitute substantial cyber incidents, and, absent this exclusion, could be considered a covered cyber incident, subject to reporting under the proposed CIRCIA regulation if an impacted customer was a covered entity. However, because such a substantial cyber incident would have been perpetrated in good faith pursuant to a penetration test duly authorized by the information system’s owner or operator (even if the owner or operator is not the sole impacted entity), neither the covered entity nor the service provider would be required to report the incident.

Conversely, circumstances could occur where a covered entity or the information system’s owner or operator authorizes an action that results in a reportable impact despite the immediately precipitating action being approved by the covered entity or information system’s owner or operator. For instance, if a covered entity, in response to a ransomware attack or other malicious incident, decides to take an action itself resulting in reportable level impacts, such as shutting down a portion of its system or operations, to prevent possibly more significant impacts, this would still be considered

¹⁴⁹ See, e.g., CISA, *Vulnerability Disclosure Policy Template* (“Only use exploits to the extent necessary to confirm a vulnerability’s presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.”), available at <https://www.cisa.gov/vulnerability-disclosure-policy-template-0>.

a reportable substantial cyber incident. In such a case, because the cyber incident itself was not perpetrated in good faith, and the threshold level impacts would not have occurred but for the initial cyber incident, CISA would not consider the covered entity’s actions to meet the “good faith” exception even though the covered entity directed the immediately precipitating action in a good faith attempt to minimize the potential impacts of a cyber incident.

iii. The Threat of Disruption as Extortion, as Described in 6 U.S.C. 650(22)

Section 681b(c)(2)(C)(ii) of title 6, United States Code, provides that the description of the types of substantial cyber incidents that constitute covered cyber events shall exclude “the threat of disruption as extortion, as described in section 2240(14)(A).” CISA is proposing incorporating this exclusion verbatim into the proposed definition of substantial cyber incident with a minor technical correction to include the updated citation to the definition for ransomware attack in CIRCIA.¹⁵⁰

Section 650(22) of title 6, United States Code, defines “ransomware attack” as “an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment.” While, as noted above, the definition of cyber incident excludes incidents where jeopardy is “imminent” but not “actual,” the definition of ransomware attack includes threatened disruptions as a means of extortion. This exclusion clarifies that the threat of disruption of a system to extort a ransom payment that does not result in the actual disruption of a system is an “imminent,” but not “actual,” event, and is therefore not required to be reported as a covered cyber incident.

However, if a covered entity makes a ransom payment in response to such a

¹⁵⁰ The definition of ransomware attack contained in Section 2240(14)(A) moved locations within the U.S. Code as part of the consolidation of definitions in the CISA Technical Corrections, *supra* note 135. While the CISA Technical Corrections did not update this cross-reference in CIRCIA, pursuant to the rule of construction in Section (f)(2) of the CISA Technical Corrections, CISA considers 6 U.S.C. 650 as the proper citation for the definition of “ransomware attack” for purposes of the proposed regulation.

threat, even if the disruption never materializes into a substantial cyber incident subject to covered cyber incident reporting required by this Part, the payment itself would still be subject to ransom payment reporting required by this Part. Only such a threat where no ransom payment is made and the disruption never materializes into a substantial cyber incident would remain excluded from mandatory reporting. Additionally, as noted in Section IV.A.ii.3.a.i above, this exclusion would not prevent a cyber incident involving a threat to disclose information obtained from an information system without authorization from being a reportable substantial cyber incident if the cyber incident otherwise meets the threshold for being a substantial cyber incident, *e.g.*, under prong (a)(1) of the substantial cyber incident definition due to the initial loss of confidentiality of the information system.

e. Examples of Cyber Incidents That Meet the Definition of Substantial Cyber Incident

To help covered entities determine what might and might not be considered a substantial cyber incident under the proposed definition, CISA is providing the following examples of (a) cyber incidents that are likely to be considered substantial cyber incidents, and (b) cyber incidents that are unlikely to be considered substantial cyber incidents. Both of these lists are for exemplary purposes only and are not intended to be exhaustive. Moreover, inclusion on either list is not a formal declaration that a similar incident would or would not be a substantial cyber incident if the agency were to finalize the definition as proposed. Inclusion here simply indicates the relative likelihood that such an incident would or would not rise to the level of a reportable substantial cyber incident. Determinations as to whether a cyber incident qualifies as a substantial cyber incident would need to be made on a case-by-case basis considering the specific factual circumstances surrounding the incident. Note, CISA continues to encourage reporting or sharing of information about all cyber incidents, even if it would not be required under the proposed regulations.

Examples of Incidents That Likely Would Qualify as Substantial Cyber Incidents

(1) A distributed denial-of-service attack that renders a covered entity's service unavailable to customers for an extended period of time.

(2) Any cyber incident that encrypts one of a covered entity's core business systems or information systems.

(3) A cyber incident that significantly increases the potential for a release of a hazardous material used in chemical manufacturing or water purification.

(4) A cyber incident that compromises or disrupts a BES cyber system that performs one or more reliability tasks.

(5) A cyber incident that disrupts the ability of a communications service provider to transmit or deliver emergency alerts or 911 calls, or results in the transmission of false emergency alerts or 911 calls.

(6) The exploitation of a vulnerability resulting in the extended downtime of a covered entity's information system or network.

(7) A ransomware attack that locks a covered entity out of its industrial control system.

(8) Unauthorized access to a covered entity's business systems caused by the automated download of a tampered software update, even if no known data exfiltration has been identified.

(9) Unauthorized access to a covered entity's business systems using compromised credentials from a managed service provider.

(10) The intentional exfiltration of sensitive data in an unauthorized manner for an unauthorized purpose, such as through compromise of identity infrastructure or unauthorized downloading to a flash drive or online storage account.

Examples of Incidents That Likely Would Not Qualify as Substantial Cyber Incidents

(1) A denial-of-service attack or other incident that only results in a brief period of unavailability of a covered entity's public-facing website that does not provide critical functions or services to customers or the public.

(2) Cyber incidents that result in minor disruptions, such as short-term unavailability of a business system or a temporary need to reroute network traffic.

(3) The compromise of a single user's credential, such as through a phishing attempt, where compensating controls (such as enforced multifactor authentication) are in place to preclude use of those credentials to gain unauthorized access to a covered entity's systems.

(4) Malicious software is downloaded to a covered entity's system, but anti-virus software successfully quarantines the software and precludes it from executing.

(5) A malicious actor exploits a known vulnerability, which a covered

entity has not been able to patch but has instead deployed increased monitoring for TTPs associated with its exploitation, resulting in the activity being quickly detected and remediated before significant additional activity is undertaken.

f. Considerations

In 6 U.S.C. 681b(c)(2)(B), Congress identified three considerations for CISA in deciding what types of substantial cyber incidents constitute covered cyber incidents. Specifically, Congress instructed CISA to consider "(i) the sophistication or novelty of the tactics used to perpetrate such a cyber incident, as well as the type, volume, and sensitivity of the data at issue; (ii) the number of individuals directly or indirectly affected or potentially affected by such a cyber incident; and (iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers." 6 U.S.C. 681b(c)(2)(B).

Throughout the process of analyzing what types of cyber incidents should constitute a substantial cyber incident, CISA kept in mind the considerations enumerated by Congress in 6 U.S.C. 681b(c)(2)(B). Some of the considerations are directly reflected in what CISA believes will be a substantial cyber incident under the proposed definition. For instance, as discussed above, factors such as the type, volume, and sensitivity of the data at issue, or the number of individuals directly or indirectly affected by an incident, will impact whether an incident should be considered a substantial cyber incident. Incidents where less data is impacted, the impacted data is not particularly sensitive, and/or the number of individuals directly or indirectly affected, are less likely to be considered substantial cyber incidents. Conversely, incidents involving large volumes of impacted data, sensitive data, or large numbers of impacted individuals are more likely to be considered substantial cyber incidents. Similarly, incidents that impact industrial control systems are much more likely to result in the second prong of the substantial cyber incident definition being met than incidents that solely impact business systems.

There is one consideration listed in 6 U.S.C. 681b(c)(2)(B), however, that CISA considered, but ultimately determined should not affect whether a cyber incident rises to the level of a substantial cyber incident in this proposed rule. That is the consideration listed in 6 U.S.C. 681b(c)(2)(B)(i), "the

sophistication or novelty of the tactics used to perpetrate such a cyber incident.” CISA believes there is value in receiving reports on all types of substantial cyber incidents, whether the tactics used are sophisticated or not, novel or not. If an unsophisticated TTP is being used to cause substantial impacts to covered entities, CISA believes there is value in knowing that so CISA and its Federal partners can warn other potential victims that this tactic is being used and can identify and share new or previously identified methods to mitigate vulnerabilities that allow this tactic to be effective.

Similarly, if there is a resurgence in adversary use of a TTP that has previously been reported upon, there is value in CISA knowing that so it can alert entities to make sure they are maintaining effective defensive measures to counter that tactic. In fact, CISA routinely adds older vulnerabilities to the Known Exploited Vulnerability database that CISA publishes based on the fact that the previously identified vulnerabilities are actively being exploited. This allows CISA and others to emphasize with the public the importance of addressing those vulnerabilities.

Finally, it is possible that neither CISA nor the reporting entity might know the sophistication or novelty of the TTP at the time of reporting. CISA and/or the reporting entity may need time to assess the incident before being able to determine its sophistication and novelty, and CISA does not believe reporting should be delayed simply to evaluate the tactics used to perpetrate a cyber incident. For the aforementioned reasons, CISA is proposing that the relative sophistication or novelty of a TTP used in perpetrating a cyber incident should not influence whether that incident meets the definition of a substantial cyber incident.

g. Harmonization of Definition With the CIRC Model Definition and Other Regulatory Definitions

As discussed in Section III.B of this document, a number of different Federal departments and agencies oversee regulations, directives, or other programs that require certain entities to report cyber incidents. CISA has received many comments from stakeholders encouraging CISA to harmonize the CIRCIA reporting requirements with the requirements in other regulations, to include the definition of what is a reportable incident. See Section III.F.x of this document. CISA fully supports the harmonization of regulatory requirements where practicable and has

been an active participant in the CIRC’s efforts to identify potential approaches to harmonizing Federal regulatory cyber incident reporting requirements. One of the specific recommendations made by the Department in its CIRC-informed Report to Congress is for departments and agencies to consider adopting a model definition for a reportable cyber incident where practicable.¹⁵¹

Cognizant of that recommendation and the value in seeking harmonization where practical, CISA considered the CIRC Model Definition for a reportable cyber incident during the development of the proposed CIRCIA definition for a substantial cyber incident. Ultimately, CISA did elect to incorporate many aspects of the CIRC Model Definition into the proposed CIRCIA definition for a substantial cyber incident, some verbatim. CISA did not propose using the CIRC Model Definition in its entirety, however, due in part to specific statutory requirements imposed within CIRCIA and the specific purposes CIRCIA is designed to achieve.

One example of where CISA’s proposed definition differs from the CIRC Model Definition due to specific language contained in CIRCIA is in the sentence used to introduce the threshold criteria that elevate an incident to the level of a reportable or substantial cyber incident. Specifically, the first sentence of the CIRC Model Definition states “[a] reportable cyber incident is an incident that leads to, or, if still under the covered entity’s investigation, could reasonably lead to any of the following [impacts].”¹⁵² The section of CIRCIA related to substantial cyber incidents states that for a cyber incident to be a substantial cyber incident, it “requires the occurrence of” one of the enumerated impacts. 6 U.S.C. 681b(c)(2)(A). Because CIRCIA requires actual occurrence of the impacts, CISA does not propose including the phrase “or, if still under the covered entity’s investigation, could reasonably lead to any of the following” in the initial sentence of the CIRCIA definition for substantial cyber incident. For similar reasons, CISA did not propose inclusion of the CIRC Model Definition’s fourth threshold prong “potential operational disruption” (emphasis added), as CISA interprets CIRCIA to require actual impact, not potential impact, for an

incident to be a substantial cyber incident.

Another substantive difference between the CIRC Model Definition and the CIRCIA proposed definition for substantial cyber incident is the inclusion in the CIRCIA proposed definition of a separate threshold prong based on a serious impact to safety and resiliency of a covered entity’s operational systems and processes. While the CIRC Model Definition does not include a similar threshold prong, this threshold is specifically listed in CIRCIA as one of the minimum types of impacts that would qualify a cyber incident for inclusion as a covered cyber incident. 6 U.S.C. 681b(c)(2)(A)(i). Accordingly, CISA determined it was important to include that impact as a basis for coverage in its definition of substantial cyber incident despite its absence in the CIRC Model Definition.

CISA also occasionally modified the language used in the CIRC Model Definition to terminology that is consistent with CIRCIA and other portions of the proposed CIRCIA regulation. For example, CISA proposes using the term “covered entity’s information system” instead of the CIRC Model Definition’s construction “a covered information system” in the first threshold prong of the definition. Because CIRCIA does not distinguish between covered and not covered information systems, networks, or technologies, the use of the word “covered” in this manner would be inconsistent.

In addition to the CIRC Model Definition, CISA also considered how other Federal regulations defined reportable cyber incidents. While many of the regulations CISA reviewed have some similarities in how they define and interpret what is a reportable cyber incident, the specific language, structure, examples, and actual requirements varied greatly based on the specific agency mission and purpose of the regulation. As the CIRC was established to make recommendations on how to harmonize these disparate regulations, and the DHS Report specifically recommends that agencies evaluate the feasibility of adapting current and future cyber incident reporting requirements to align with a model definition of a reportable cyber incident,¹⁵³ CISA ultimately felt that the path that would most effectively support harmonization across the various Federal cyber incident reporting requirements was to align the definition of covered cyber incident, to the extent

¹⁵¹ *DHS Report*, *supra* note 4, at 25 (“Recommendation 1: The Federal Government should adopt a model definition of a reportable cyber incident wherever practicable. Federal agencies should evaluate the feasibility of adapting current and future cyber incident reporting requirements to align to a model definition of a reportable cyber incident.”).

¹⁵² *Id.* at 26.

¹⁵³ *Id.* at 25–27.

practicable, with the CIRC Model Definition.

iii. CIRCIA Reports

1. CIRCIA Report

CISA is proposing to include in the regulation a definition of the term CIRCIA Report. CIRCIA requires a covered entity to submit (either directly or through a third party) a report to CISA when it reasonably believes a covered cyber incident occurred, makes a ransom payment, or experiences one of a number of circumstances that requires the covered entity to update or supplement a previously submitted Covered Cyber Incident Report. 6 U.S.C. 681b(a)(1)–(3). These reports are called Covered Cyber Incident Reports, Ransom Payment Reports, and Supplemental Reports, respectively. CIRCIA additionally allows covered entities that make a ransom payment associated with a covered cyber incident to submit a single report to satisfy both the covered cyber incident and ransom payment reporting requirements. 6 U.S.C. 681b(a)(5)(A). CISA is proposing to call this joint submission a Joint Covered Cyber Incident and Ransom Payment Report.

CISA is proposing a term CIRCIA Report to be an umbrella term that encompasses all four types of covered entity reports collectively. Accordingly, CISA is proposing to define CIRCIA Report to mean a Covered Cyber Incident Report, Ransom Payment Report, Joint Covered Cyber Incident and Ransom Payment Report, or Supplemental Report.

In some instances, CIRCIA refers to “reports,” and at other times refers to “information” (either information contained in a CIRCIA Report or information about cyber incidents, covered cyber incidents, or ransom payments). CISA understands Congress’ use of these different terms in different contexts within CIRCIA to be intentional, and therefore replicates these distinctions in the proposed rule. Specifically, references to a CIRCIA Report or any individual report (*i.e.*, a Covered Cyber Incident Report, Ransom Payment Report, Joint Covered Cyber Incident and Ransom Payment Report, or Supplemental Report) throughout this NPRM are intended to refer to the submission as a whole. By contrast, references to information (either in a CIRCIA Report or about cyber incidents, covered cyber incidents, or ransom payments) are intended to refer to discrete pieces of facts and ideas (which sometimes may be contained within a CIRCIA Report, perhaps along with

other pieces of information), rather than the submission as a whole.

2. Covered Cyber Incident Report

CISA is proposing to include in the regulation a definition of the term Covered Cyber Incident Report. CIRCIA requires a covered entity that experiences a covered cyber incident to report that incident to CISA. 6 U.S.C. 681b(a)(1). CISA is proposing to refer to this type of report as a Covered Cyber Incident Report and to define that term to mean a submission made by a covered entity or a third party on behalf of a covered entity to report a covered cyber incident as required by this Part. CISA is further proposing that a Covered Cyber Incident Report also includes any additional, optional information submitted as part of a Covered Cyber Incident Report.

As noted in the definition, a Covered Cyber Incident Report may be submitted by a covered entity or by a third party on behalf of a covered entity. Additionally, a covered entity may voluntarily include within a Covered Cyber Incident Report additional information pursuant to 6 U.S.C. 681c(b). Voluntarily provided information will be considered part of the Covered Cyber Incident Report. Additional requirements related to the manner, form, content, and other aspects of a Covered Cyber Incident Report are described in Sections IV.E.i–iii of this document and §§ 226.6, 226.7, and 226.8 of the proposed regulation.

3. Ransom Payment Report

CISA is proposing to include in the regulation a definition of the term Ransom Payment Report. CIRCIA requires a covered entity that makes a ransom payment, or has another entity make a ransom payment on the covered entity’s behalf, to report that payment to CISA. 6 U.S.C. 681b(a)(2)(A). CISA is proposing to refer to this type of report as a Ransom Payment Report and to define that term to mean a submission made by a covered entity or a third party on behalf of a covered entity to report a ransom payment as required by this Part. CISA is further proposing for a Ransom Payment Report to also include any additional, optional information submitted as part of a Ransom Payment Report.

As noted in the definition, a Ransom Payment Report may be submitted by a covered entity or by a third party on behalf of a covered entity. Additionally, a covered entity may voluntarily include within a Ransom Payment Report additional information submitted pursuant to 6 U.S.C. 681c(b). Voluntarily provided information will

be considered part of the Ransom Payment Report. Additional requirements related to the manner, form, content, and other aspects of a Ransom Payment Report are described in Sections IV.E.i–iii of this document and §§ 226.6, 226.7, and 226.9 of the proposed regulation. If the ransom payment being reported is the result of a covered cyber incident that the covered entity or a third party acting on its behalf has already reported to CISA, then the Ransom Payment Report also would be considered a Supplemental Report and must meet any requirements associated with Supplemental Reports as well.

4. Joint Covered Cyber Incident and Ransom Payment Report

CISA is proposing to include in the regulation a definition of the term Joint Covered Cyber Incident and Ransom Payment Report. Pursuant to 6 U.S.C. 681b(a)(5)(A), covered entities that make a ransom payment associated with a covered cyber incident prior to the expiration of the 72-hour reporting timeframe for reporting the covered cyber incident may submit a single report to satisfy both the covered cyber incident and ransom payment reporting requirements. CISA is proposing to call this joint submission a Joint Covered Cyber Incident and Ransom Payment Report and to define that term to mean a submission made by a covered entity or a third party on behalf of a covered entity to simultaneously report both a covered cyber incident and ransom payment related to the covered cyber incident being reported. CISA is proposing that a Joint Covered Cyber Incident and Ransom Payment Report also include any additional, optional information submitted as part of the report.

As noted in the definition, a Joint Covered Cyber Incident and Ransom Payment Report may be submitted by a covered entity or by a third party on behalf of a covered entity. Additionally, a covered entity may voluntarily include within a Joint Covered Cyber Incident and Ransom Payment Report additional information pursuant to 6 U.S.C. 681c(b). Voluntarily provided information will be considered part of the Joint Covered Cyber Incident and Ransom Payment Report. Additional requirements related to the manner, form, and content of a Joint Covered Cyber Incident and Ransom Payment Report are described in Sections IV.E.i–iii of this document and §§ 226.6, 226.7, and 226.10 of the proposed regulation.

5. Supplemental Report

CISA is proposing to include in the regulation a definition of the term Supplemental Report. CIRCIA requires a covered entity to promptly submit an update or supplement to a previously submitted Covered Cyber Incident Report under certain circumstances. 6 U.S.C. 681b(a)(3). CISA is proposing to refer to this type of report as a Supplemental Report. CISA is proposing that the term Supplemental Report be used to describe a submission made by a covered entity or a third party on behalf of a covered entity to update or supplement a previously submitted Covered Cyber Incident Report or to report a ransom payment made by the covered entity after submitting a Covered Cyber Incident Report as required by this Part. CISA is further proposing that a Supplemental Report also include any additional, optional information submitted as part of a Supplemental Report.

As noted in the definition, a Supplemental Report may be submitted by a covered entity or by a third party on behalf of a covered entity. Additionally, a covered entity may voluntarily include within a Supplemental Report additional information pursuant to 6 U.S.C. 681c(b). Voluntarily provided information is considered part of the Supplemental Report. Additional requirements related to the manner, form, content, and other aspects of a Supplemental Report are described in Sections IV.E.i–iii of this document and §§ 226.6, 226.7, and 226.11 of the proposed regulation.

iv. Other Definitions

1. CIRCIA

CISA is proposing to define the term CIRCIA to mean the Cyber Incident Reporting for Critical Infrastructure Act of 2022, as amended. This will simplify the regulatory text by allowing CISA to refer to CIRCIA without having to use the full title of the statute or full legal citation throughout the regulation.

2. CIRCIA Agreement

CISA is proposing to create the term CIRCIA Agreement and define it as an agreement between CISA and another Federal agency that meets the requirements of § 226.4(a)(2), that has not expired or been terminated, and which, when publicly posted in accordance with § 226.4(a)(5), indicates the availability of a substantially similar reporting exception. CISA believes the establishment and defining of this term will allow covered entities to better identify circumstances where they can

leverage the substantially similar reporting exception and avoid potentially duplicative reporting to another Federal department or agency and CISA. Additional details on both the CIRCIA Agreement and the substantially similar reporting exception can be found in Section IV.D.i of this document.

3. Cloud Service Provider

CISA is proposing to include a definition for the term cloud service provider. CISA believes defining this term is important to ensure that covered entities understand the meaning of an unauthorized access or disruption of business or industrial operations due to a loss of service facilitated through, or caused by, a compromise of a CSP, as that is one example of a substantial cyber incident provided in CIRCIA. 6 U.S.C. 681b(c)(2)(A)(iii). Section 650 of title 6, United States Code, defines the term CSP as “an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.” 6 U.S.C. 650(3). Because this definition applies to all of Title XXII of the Homeland Security Act of 2002, as amended, including CIRCIA, CISA is proposing to use this definition in the regulation.

4. Cybersecurity and Infrastructure Security Agency (CISA)

CISA is proposing to include a definition for the term Cybersecurity and Infrastructure Security Agency or CISA. This term is used repeatedly throughout the proposed regulation to describe the Federal entity responsible for the oversight of the proposed CIRCIA regulation and with whom covered entities and other stakeholders will engage on various activities required under the regulation. CISA is proposing to define Cybersecurity and Infrastructure Security Agency or CISA as the Cybersecurity and Infrastructure Security Agency as established under section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652), as amended by the Cybersecurity and Infrastructure Security Agency Act of 2018 and subsequent laws, or any successor organization.

5. Cybersecurity Threat

CISA is proposing to include a definition for the term cybersecurity threat. Defining the term cybersecurity threat is a streamlined approach that provides needed context for the requirement in 6 U.S.C. 681b(c)(8)(D) that CISA include in the final rule

procedures for, among other things, protecting privacy and civil liberties, for certain personal information received in CIRCIA Reports that is not directly related to a cyber threat. For the reasons explained below, CISA is proposing to use and define the term cybersecurity threat instead of “cyber threat.”

CIRCIA defines the term “cyber threat” as “ha[ving] the meaning given the term ‘cybersecurity threat’ in section 2200 [6 U.S.C. 650]” of the Homeland Security Act of 2002, as amended. Section 650 of title 6, United States Code, defines “cybersecurity threat” as “an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system,” other than “any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.” 6 U.S.C. 650(8). Rather than using the term “cyber threat,” CISA is proposing to use the term “cybersecurity threat,” with this definition effectively verbatim, because CISA believes it is most consistent with CIRCIA.

6. Director

CISA is proposing to include a definition for the term Director and to define it as the Director of CISA, any successors to that position, or any designee. CISA is proposing to include this definition as CIRCIA assigns the Director specific responsibilities related to implementation of the CIRCIA regulation.

7. Information System

CISA is proposing to include a definition for the term information system. This term is a key term for the proposed regulation as, among other things, it is used within the definition of ransomware attack and substantial cyber incident as well as to help identify the types of information that a covered entity must provide in reports required under the regulation.

The Paperwork Reduction Act of 1980 (PRA), 44 U.S.C. 3502, defines information system as “a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.”¹⁵⁴ Section 650 of title 6, United States Code, defines information system as having the meaning given the term in the PRA,

¹⁵⁴ 44 U.S.C. 3502(8).

44 U.S.C. 3502, specifically including “industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.” 6 U.S.C. 650(14).

Because the 6 U.S.C. 650 definition applies to all of Title XXII of the Homeland Security Act of 2002, as amended, including CIRCIA, CISA is proposing defining Information using the language contained in the definition in 6 U.S.C. 650(14) with the addition of an explicit acknowledgment that OT is included within the definition of information system. CISA believes OT is encompassed in the definition of information system contained within 6 U.S.C. 650(14) by reference to industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; however, CISA is proposing to explicitly include the words “operational technology systems” within the definition in light of the common industry use of this term to avoid any potential misinterpretations about whether OT is encompassed by the proposed CIRCIA definition of information systems.

8. Managed Service Provider

CISA is proposing to include a definition for the term managed service provider. CISA believes it is important to define this term to ensure that covered entities understand the meaning of an unauthorized access or disruption of business or industrial operations due to a loss of service facilitated through, or caused by, a compromise of a managed service provider, as that is one example of a substantial cyber incident provided in CIRCIA. 6 U.S.C. 681b(c)(2)(A)(iii). The term managed service provider is defined in 6 U.S.C. 650(18) and sets out three criteria that must be met to qualify as a managed service provider. The definition reads, “an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.” 6 U.S.C. 650(18). Because this definition applies to all of Title XXII of the Homeland Security Act of 2002, as amended, including CIRCIA, CISA is proposing to use this same definition of managed service provider in the regulation.

9. Personal Information

CISA is proposing to include a definition for the term personal

information. Personal information is a key term in the proposed regulation as CIRCIA requires CISA to undertake certain steps to protect personal information. See *e.g.*, 6 U.S.C. 681e(a)(3). CISA is proposing to define the term personal information to mean information that identifies a specific individual or information associated with an identified or identifiable individual. Under this definition, personal information would include, but are not limited to, both identifying information such as photographs, names, home addresses, direct telephone numbers, and Social Security numbers as well as information that does not directly identify an individual but is nonetheless personal, nonpublic, and specific to an identified or identifiable individual. Examples would include medical information, personal financial information (*e.g.*, an individual’s wage or earnings information; income tax withholding records; credit score; banking information), contents of personal communications, and personal web browsing history. This proposed definition would include “personally identifiable information,” as defined in OMB Memorandum M–17–12 as referring to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual, but also proposes to include information that might not be clearly linkable to an individual but would nonetheless relate to a specific individual and be considered personal and nonpublic, such as an individual’s web browsing history or the content of an email. CISA is proposing this definition to encompass the broad range of personally sensitive information that a cybersecurity incident might implicate, including the content of personal communications, which might not be able to be used on its own to identify an individual, to ensure that all personally sensitive information is handled appropriately.

CISA is not proposing to include in this definition information that does not relate to a specific individual. Therefore, information such as general business telephone numbers or business financial information would generally not be considered personal information under this definition.

This proposed definition of “personal information” would be different and broader than the approach taken by the Cybersecurity Information Sharing Act of 2015, (6 U.S.C. 1501 *et seq.*). 6 U.S.C. 1503(d)(2) more narrowly requires removal of information that is “known

at the time of sharing” to be “personal information” that identifies a specific person or belongs to a specific person rather than information that is linked or linkable to a specific person. CISA welcomes public comment on this proposed definition of “personal information” and whether CISA should instead adopt the approach taken by the Cybersecurity Information Sharing Act of 2015 to defining personal information.

10. Ransom Payment

CISA is proposing to include a definition for the term ransom payment. Ransom payment is a key term in the proposed regulation as CIRCIA requires that covered entities report ransom payments to CISA within 24 hours of the payment being made. 6 U.S.C. 681b(a)(2). CISA is proposing to use the definition of the term ransom payment from CIRCIA in the regulation verbatim.

11. Ransomware Attack

CISA is proposing to include a definition for the term ransomware attack. CIRCIA requires a covered entity that makes a ransom payment as the result of a ransomware attack to report the ransom payment to CISA within 24 hours of making the payment. 6 U.S.C. 681b(a)(2). CISA believes including a definition for the term ransomware attack will help covered entities determine whether they are required to submit a Ransom Payment Report to CISA.

Section 650(22) of title 6, United States Code, defines the term ransomware attack as “(A) [] an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and (B) does not include any such event where the demand for payment is (i) not genuine; or (ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system.” 6 U.S.C. 650(22). Because this definition applies to all of Title XXII of the Homeland Security Act of 2002, as amended, including CIRCIA, CISA is proposing to use this definition with a few minor modifications described below.

First, in defining the term ransomware attack, CISA is proposing to replace the term “incident” (which is

used in the statutory definition of ransomware attack) with the full definition of “incident” as found in section 2200(12) of the Homeland Security Act of 2002, as amended (6 U.S.C. 650(12)) (*i.e.*, “an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system”). The definition of “incident” in 6 U.S.C. 650(12) applies to the term “incident” throughout Title XXII of the Homeland Security Act of 2002, as amended, including to the term “incident” within the statutory definition of ransomware attack at 6 U.S.C. 650(22).¹⁵⁵

Using this definition of “incident” is not only consistent with the statute, but it also avoids CISA specifically defining the term “incident” in the regulation, which CISA believes could create confusion in light of the inclusion in the proposed regulation of a definition for the term cyber incident.

CISA considered, but ultimately decided against, proposing the use of the term “cyber incident” in place of “incident” in the definition of ransomware attack. As noted earlier in the discussion of the proposed definition for cyber incident, CIRCIA removed the “imminently jeopardizes” clause found in the Homeland Security Act’s definition of “incident” from CIRCIA’s definition of cyber incident, instead opting to require “actual jeopardy” for an event to qualify as a cyber incident under CIRCIA. Consequently, using the term “cyber incident” in lieu of “incident” in the definition of ransomware attack would have a substantive impact on the definition. CISA believes that Congress intentionally used the term “incident” (in lieu of the term “cyber incident”) in the definition of ransomware attack to account for the fact that a ransomware attack may involve a threat of disruption (*i.e.*, imminent jeopardy) and that such

a threat—without the disruption ever occurring—may be sufficient to extort a ransom payment. Moreover, Congress specifically included incidents where jeopardy is “imminent” but not “actual” in its definition of ransomware attack, including both threatened and realized interruptions as means of extortion. Therefore, to avoid a substantive change to the meaning of the term ransomware attack (which would also narrow the scope of reportable ransom payments), while also avoiding the confusion that could be caused by similarly defining both “cyber incident” and “incident” in the proposed rule, the proposed rule relies on 6 U.S.C. 650(12)’s definition of the word “incident” in lieu of the word “incident” within the definition of the term ransomware attack.

Second, the NPRM replaces the word “includes” with “involves, but need not be limited to, the following.” This change was made to avoid the implication that the term ransomware attack includes some other category of incidents not otherwise described here (*i.e.*, that “includes” means “includes, but is not limited to”). At the same time, the definition is not intended to suggest that any occurrence that includes more than the three listed elements is no longer considered a ransomware attack. The “need not be limited to” clause is intended to convey that, as long as the three listed elements are involved in the occurrence in question, any additional facts about the occurrence would not cause it to be outside of the definition of a ransomware attack.

Third, CISA is proposing to delete the phrase “a demand” from the third prong of the statutory definition, thus modifying it from “to extort a demand for a ransom payment” to “to extort a ransom payment.” This is intended to clarify that this prong requires that the threat actor extort the ransom payment itself from the victim (consistent with the common understanding of a typical ransomware attack), and not a process where the extortion is a demand for the victim entity to demand a ransom payment from a third entity. This interpretation is supported by the legislative history of CIRCIA showing that Congress understood this term to encompass the traditional ransomware attacks that the country was experiencing at a significantly increasing frequency in the months and years prior to CIRCIA’s passage¹⁵⁶ and

not a novel two-step extortion of a demand that, to CISA’s knowledge, has never occurred. Numerous canons of statutory interpretation, to include the Absurdity Doctrine, the Harmonious-Reading Canon, and the canon of Purposive Construction, further support this interpretation.

CISA’s proposed definition also includes two minor, non-substantive changes to improve the readability of the definition. First, CISA is proposing to separate the statutory description of the type of incident that constitutes a ransomware attack into three subparts, one for each of the three prongs of the definition. Second, in the portion of the statutory definition contained in the newly delineated paragraph (1), CISA is proposing to eliminate the second instance of the phrase “use or threat of use” and instead insert roman numerals and the conjunction “or” to make clear that the “use or threat of use” phrase applies to both (i) unauthorized or malicious code on an information system or (ii) another digital mechanism such as a denial-of-service attack.

The proposed definition of ransomware attack contains language mirroring language in the CIRCIA authorizing legislation that excludes from the definition any event where the demand for a ransom payment is “not genuine” or is “made in good faith by an entity in response to a specific request by the owner or operator of the information system.” Circumstances in which an entity may determine a ransom demand is “not genuine” include if the demand is a known hoax or the demand lacks necessary information for the receiving entity to comply, such as an amount demanded or payment instructions. Ransom

ensure that CISA has the visibility it needs to help defend our Federal networks and to help our critical infrastructure owners and operators protect themselves.”), (statement of Rep. John Katko, Ranking Member, H. Comm. on Homeland Security) (“Every single day, entities, large and small, are affected by the scourge of ransomware. . . .”); 168 Cong. Rec. S1149–50 (daily ed. Mar. 14, 2022) (statement of Sen. Mark Warner) (“[R]ansomware attacks are a serious national security threat that have affected everything from our energy sector to the Federal Government and Americans’ own sensitive information. . . . As . . . ransomware attacks continue to increase, the Federal Government must be able to quickly coordinate a response and hold bad actors accountable.”); HSGAC Minority Staff Report, *America’s Data Held Hostage: Case Studies in Ransomware Attacks on American Companies* at iii (“Ransomware is a type of malware that encrypts victims’ computer systems and data, rendering the systems unusable and the data unreadable. Perpetrators then issue a ransom demand. . . . If the victim pays, hackers may provide the victim with a key to decrypt their systems and data. . . .” (italics in original)), available at <https://www.hsgac.senate.gov/library/files/americas-data-held-hostage-case-studies-in-ransomware-attacks-on-american-companies/>.

¹⁵⁵ As originally enacted, CIRCIA explicitly included a definition of both “cyber incident” and “incident.” See Public Law 117–103. However, when the definition of “incident” was moved as part of the consolidation of definitions in the CISA Technical Corrections to the beginning of Title XXII of the Homeland Security Act (6 U.S.C. 650(12)), the definition of “incident” in CIRCIA was struck as a conforming edit to remove the redundancy. See CISA Technical Corrections, *supra* note 135, Section (b)(2)(N)(v). Further, in the original as-enacted version of CIRCIA, both uses of the term “incident” (as opposed to the CIRCIA term “cyber incident”) were in definitions that were moved to 6 U.S.C. 650 as part of the CISA Technical Corrections, namely the definitions of ransomware attack and supply chain compromise. See 6 U.S.C. 650(22) and (28).

¹⁵⁶ See, e.g., *Stakeholder Perspectives Hearing*, *supra* note 17, at 12–13 (statement of Rep. Andrew Garbino, Ranking Member, Subcomm. on Cybersecurity, Infrastructure Protection, and Innovation of the H. Comm. on Homeland Security) (“Everyone here remembers the ransomware attacks on Colonial Pipeline and JBS Meats. . . . We must

demands “made in good faith by an entity in response to a specific request by the owner or operator of the information system” typically would include those that are part of red teaming, penetration testing, vulnerability analysis, training exercises, or other authorized activities designed to test prevention, detection, response, or other capabilities of the requesting entity. In both exclusions, while there may facially be a demand that would otherwise meet the definition of ransomware attack, the demand is made without expectation or desire to actually receive a ransom payment from the covered entity. Similar to the parallel “good faith” exclusion in the definition of substantial cyber incident (as discussed in Section IV.A.ii.3.d.ii of this document), because the exception only applies to instances where the demand for ransom payment was made “in response to a specific request by” the information system owner or operator, this exception would only apply to situations where the request or authorization preceded the demand for ransom payment.

It is noteworthy that, though the definition of a ransomware attack specifically addresses cyber incidents involving interruption or disruption of operations and threats to do the same, it does not include other forms of extortionate cyber incidents that are similar to ransomware attacks; specifically, extortionate demands for payment based on threats to leak sensitive information obtained without authorization from an information system. While such incidents (without more) do not fall within the definition of a ransomware attack, they would still be reportable under CIRCIA, if the incident otherwise qualifies as a covered cyber incident, as proposed to be defined in § 226.1, *e.g.*, if the underlying incident (including any actual disclosure in line with those threats) leads to the substantial loss of confidentiality of an information system or network.

12. State, Local, Tribal, or Territorial Government Entity

CISA is proposing to include a definition for the term State, Local, Tribal, or Territorial Government entity. This term has significance in the regulation for two primary reasons. First, the term is used within the proposed definition of covered entity to describe certain entities that would be subject to CIRCIA’s reporting requirements. Second, pursuant to 6 U.S.C. 681d(f), the section of CIRCIA on noncompliance with required reporting

does not apply to a SLTT Government entity.

The U.S. Census Bureau defines a government entity as “an organized entity which, in addition to having governmental character, has sufficient discretion in the management of its own affairs to distinguish it as separate from the administrative structure of any other governmental unit.”¹⁵⁷ The Homeland Security Act definition for the term “State” includes both States and territories, defining the term “State” to mean “any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.” 6 U.S.C. 101(17). The Homeland Security Act definition for the term “Local Government” includes both local and tribal government entities, defining the term “Local Government” to mean “(a) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a Local government; (b) An Indian tribe or authorized tribal organization, or in Alaska, a Native village or Alaska Regional Native Corporation; and (c) A rural community, unincorporated town or village, or other public entity.” 6 U.S.C. 101(13).

To create its proposed definition for the term SLTT Government entity, CISA is proposing to create an umbrella term that merges the three definitions referenced in the previous paragraph, and include the definition of Indian tribe that is referenced in the Homeland Security Act. This approach will allow CISA to leverage existing, accepted definitions for each element that composes the term SLTT Government entity—*i.e.*, State, local, territorial, tribal, and government entity—within a single, consolidated definition. CISA believes this is also appropriate because SLTT Government Entities are treated the same throughout the proposed regulation, and this umbrella term simplifies this task.

13. Supply Chain Compromise

CISA is proposing to include a definition for the term supply chain

compromise. This term has significance in the regulation as CIRCIA explicitly states that unauthorized access facilitated through or caused by a supply chain compromise can be a substantial cyber incident. See 6 U.S.C. 681b(c)(2)(A)(iii).

Section 650 of title 6, United States Code defines “supply chain compromise” as “an incident within the supply chain of an information system that an adversary can leverage, or does leverage, to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.” 6 U.S.C. 650(28). NIST defines a “supply chain” as the “linked set of resources and processes between and among multiple levels of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle.”¹⁵⁸ The supply chain for an information system is typically considered to be the multiple layers of software and hardware that are integrated to perform the various functions of the information system. Examples of items in the supply chain of an information system, which are acquired often from multiple vendors, include hardware items like microchips (and the components that comprise the microchips), operating systems (and the code libraries that comprise the operating systems), and other types of software (and the code libraries that compromise the software). Information systems—including both ICT and OT—“rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem that . . . consists of multiple levels of outsourcing. This ecosystem is comprised of public and private sector entities (*e.g.*, acquirers, suppliers, developers, system integrators, external service providers, and other ICT/OT-related service providers) that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilize or manage ICT/OT products and services.”¹⁵⁹

CISA is proposing to use the definition of the term supply chain compromise contained in 6 U.S.C. 650 verbatim for the definition of the term in the regulation with one exception: the definition in the proposed regulation replaces the term “incident”

¹⁵⁷ U.S. Bureau of the Census, *Classification Manual* (Oct. 2006), available at <https://www.census.gov/programs-surveys/gov-finances/technical-documentation/classification-manuals.html>.

¹⁵⁸ NIST, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, NIST Special Publication 800–161 Rev.1, at 1 (May 2022), available at <https://csrc.nist.gov/pubs/sp/800/161/r1/final>.

¹⁵⁹ See *id.*

with the term “cyber incident.” As noted in the earlier discussion on the term cyber incident, Congress narrowed the types of incidents CISA could require reporting on under CIRCIA by explicitly stating the term cyber incident did not include an incident that imminently jeopardizes, but does not actually jeopardize, an information system or the information contained therein. As the use of the term supply chain compromise in the regulation is limited to the definition of certain substantial cyber incidents, the actual (versus imminent) jeopardy requirement is built into the broader requirements already, thus making the end result the same regardless of whether the definition of supply chain compromise uses the term incident or cyber incident. Rather than introducing potential confusion into the regulation by defining incident and cyber incident, CISA is proposing to use the term cyber incident in the definition of supply chain compromise.

As noted in the definition, a supply chain compromise can occur anywhere in the lifecycle of an information system. This can include design, development and production, distribution, acquisition and deployment, maintenance, or disposal.¹⁶⁰ For example, a supply chain compromise can occur when a cyber threat actor infiltrates a software vendor’s network and deploys malicious code to compromise the software before the vendor sends it to their customers, which then compromises the customer’s data or systems.¹⁶¹ Newly acquired software or hardware may be compromised from the outset, or a compromise may occur through other means like a patch or a hotfix.¹⁶² Common techniques for software supply chain compromises include hijacking updates, undermining code signing, and compromising open source code.¹⁶³

14. Virtual Currency

CISA is proposing to include a definition for the term virtual currency. CISA is proposing to define this term because CIRCIA requires covered entities to include in any Ransom Payment Report “the type of virtual currency or other commodity requested” as part of the ransom demand. 6 U.S.C. 681b(c)(5)(G). CISA

wants to ensure that covered entities understand this requirement.

CIRCIA defines virtual currency as “the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.” 6 U.S.C. 681(10). CISA understands this definition as equivalent to a “value that substitutes for currency or funds” in 31 U.S.C. 5312(a)(2)(J), and “virtual currency” as defined in guidance from the Financial Crimes Enforcement Network (FinCEN).¹⁶⁴ Therefore, CISA is proposing to clarify the relationship between these terms by adding a sentence to the definition in CIRCIA noting that virtual currency includes any form of value that substitutes for currency or funds.

v. Request for Comments on Proposed Definitions

CISA seeks comments on all the proposed definitions. In addition, CISA seeks specific comments on the following questions:

3. The proposed definitions of cyber incident, covered cyber incident, and substantial cyber incident, to include the appropriateness and clarity of the thresholds contained in the proposed definition of substantial cyber incident, the three exclusions to the proposed definition of substantial cyber incident, and the guiding principles described in Section IV.A.ii.b of this document regarding how to determine if an incident was a substantial cyber incident.

4. Whether CISA should specifically add the term “significant,” “substantial,” or any other appropriate word at the beginning of subparagraph 3 of the definition of substantial cyber incident to clarify the impact level required.

5. The proposed examples of incidents that likely would or would not qualify as a substantial cyber incident, to include whether the examples provided by CISA are accurate and whether there are other types of incidents that it would be useful to include in the list of examples to incidents that likely would or would not qualify as a substantial cyber incident.

6. Anticipated challenges for covered entities related to understanding or reporting a covered cyber incident if such incident stemmed from a disruption of a third-party vendor or

service provider that is itself not a covered entity.

7. As noted in the preamble, CISA believes there is value in CISA receiving reports on all types of cyber incidents that meet the substantial cyber incident impact thresholds, regardless of whether the TTPs used are sophisticated or not, or novel or not. Therefore, CISA proposes that the “sophistication or novelty of the tactics” should not influence whether an individual incident or category of incidents qualifies as a substantial cyber incident. Do you agree with this proposal, or should the sophistication or novelty of a tactic influence whether an individual incident or category of incidents meets one of the substantial cyber incident thresholds? Similarly, should CISA use sophistication or novelty of a tactic as a justification for including or excluding any specific categories of incidents from the population of cyber incidents required to be reported? How does this intersect with the minimum requirements enumerated in 6 U.S.C. 681b(c)(2)(A)?

8. Should exploitation of a zero-day vulnerability as a general matter be considered to meet one of the threshold impacts in the definition of substantial cyber incident? Please provide data or information specifically regarding (1) whether exploitation of a zero-day vulnerability provides an indication of a malicious actor’s sophistication, (2) whether exploitation of a zero-day vulnerability results in a different level of risk to a victim entity than exploitation of a known vulnerability, and (3) benefits that reporting on the exploitation of zero-day vulnerabilities might provide to CISA’s understanding of the cyber threat landscape, CISA’s ability to warn entities about emerging threats, and the federal government’s awareness of victim entities targeted in cyber incidents utilizing zero-day vulnerabilities.

9. Whether there are any terms for which CISA did not propose a definition but should consider including to improve the clarity of the regulation.

B. Applicability

As noted in Section IV.A.i. above, due to the operative significance and impact of the term, CISA proposes to define covered entity to mean any entity that meets the criteria established in the Applicability Section, § 226.2. CISA believes that § 226.2 also satisfies the statutory requirement that CISA include in the final rule a “clear description of the types of entities that constitute covered entities.” See 6 U.S.C. 681b(c)(1).

¹⁶⁰ CISA, *Defending Against Software Supply Chain Attacks* at 3, available at <https://www.cisa.gov/resources-tools/resources/defending-against-software-supply-chain-attacks-0> (Apr. 2021).

¹⁶¹ *Id.* at 2.

¹⁶² See *id.*

¹⁶³ *Id.* at 4.

¹⁶⁴ FinCEN Guidance, FIN–2019–G001, *Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies* at 7 (May 9, 2019), available at <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models>.

The proposed Applicability section includes two primary means by which an entity in a critical infrastructure sector qualifies as a covered entity, the first based on the size of the entity and the second based on whether the entity meets any of the enumerated sector-based criteria. An entity in a critical infrastructure sector only needs to meet one of the criteria to be considered a covered entity. For example, an entity in a critical infrastructure sector that exceeds the size standard and meets none of the § 226.2(b) sector-based criteria will be considered a covered entity. Conversely, an entity that meets one or more of the sector-based criteria will be a covered entity regardless of whether it exceeds the § 226.2(a) size standard. An entity in a critical infrastructure sector does not have to meet both the size-based criterion and one of the sector-based criteria to be considered a covered entity.

i. Interpreting the CIRCIA Statutory Definition of Covered Entity

In developing this proposed Applicability section, CISA first looked at the parameters imposed by CIRCIA. See 6 U.S.C. 681(4). Specifically, in the definition of covered entity provided by CIRCIA, Congress limits what may be a covered entity to “an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21.” See 6 U.S.C. 681(4).

PPD-21 does not define the word “entity” but instead adopts a systems and assets approach when referring to critical infrastructure. However, this does not fit within the regulatory scheme required by CIRCIA. Therefore, CISA interprets the word “entity” to be a broad term, generally including any person, partnership, business, association, corporation, or other organization (whether for-profit, not-for-profit, nonprofit, or government) regardless of governance model that has legal standing and is uniquely identifiable from other entities.¹⁶⁵ The organizational structure or nomenclature chosen by the entity does not matter as long as it is a structure that imports legal presence or standing in

¹⁶⁵ Black’s Law Dictionary defines “entity” as “[a] generic term inclusive of person, partnership, organization, or business [that] can be legally bound [and] is uniquely identifiable from any other entity.” See Black’s Law Dictionary, 2nd Ed., as found on www.thelawdictionary.org. Black’s also contains a separate definition for “legal entity,” defining it as “[a] lawful or legally standing association, corporation, partnership, proprietorship, trust, or individual [that] has legal capacity to (1) enter into agreements or contracts, (2) assume obligations, (3) incur and pay debts, (4) sue and be sued in its own right, and (5) to be accountable for illegal activities.” *Id.*

the United States. CISA does not, therefore, interpret or understand the word “entity” to mean a system or asset, and some of the things that would not be considered entities include software, hardware, and other equipment; buildings and facilities; and systems. CISA believes this interpretation is both consistent with the plain language meaning of the term “entity” and appropriate given the purposes of CIRCIA, which require CISA to collect sufficient reports to develop analysis and understand cyber threat trends across the entire critical infrastructure landscape.

The second limitation contained in the statutory definition is that the entity must be “in a critical infrastructure sector, as defined in Presidential Policy Directive 21.” Presidential Policy Directive 21 (PPD-21) does not actually contain a definition for “critical infrastructure sector,” but it does specifically enumerate 16 critical infrastructure sectors.¹⁶⁶ PPD-21 also does not specifically define the composition of the individual critical infrastructure sectors; however, PPD-21 required the Secretary of Homeland Security to update the National Infrastructure Protection Plan (NIPP), which is intended to guide the national effort to manage risks to the Nation’s critical infrastructure. The NIPP included a “Call to Action” which required each critical infrastructure sector to update its Sector-Specific Plan (SSP) as part of an overall joint planning effort and to update the SSP every four years thereafter.¹⁶⁷ The SSPs are developed jointly by representatives of the private sector, referred to as Sector Coordinating Councils (SCCs),¹⁶⁸ and representatives of the government, referred to as Government Coordinating

¹⁶⁶ The 16 critical infrastructure sectors enumerated in PPD-21 are Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems.

¹⁶⁷ The NIPP states that SSPs are supposed to be updated every four years, but to date, none of these plans have been updated. See *National Infrastructure Protection Plan* (2013), available at <https://www.cisa.gov/resources-tools/resources/2013-national-infrastructure-protection-plan>.

¹⁶⁸ The SCCs are self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. The SCCs coordinate and collaborate with SRMAs and related Government Coordinating Councils to address the entire range of critical infrastructure security and resilience policies and efforts for that sector. See <https://www.cisa.gov/resources-tools/groups/sector-coordinating-councils> (last visited Nov. 28, 2023).

Councils (GCCs).¹⁶⁹ Each SSP¹⁷⁰ includes a “sector profile,” which describes entities that are in the respective critical infrastructure sector. These profiles do not limit the descriptions of the entities that comprise each critical infrastructure sector identified in PPD-21 to entities that own systems and assets that meet the statutory definition of “critical infrastructure” set forth by 42 U.S.C. 5195c(e).¹⁷¹ Rather, in implementing PPD-21, the SSPs make clear that a wide variety of entities, including at least some entities that do not own or operate systems or assets that meet the definition of critical infrastructure in PPD-21 but are active participants in critical infrastructure sectors and communities, are considered “in a critical infrastructure sector.”

For example, according to the 2015 Food and Agriculture SSP, among the variety of entities that composed the Food and Agriculture Sector in 2014 were more than 935,000 restaurants and institutional food service establishments; an estimated 114,000 supermarkets, grocery stores, and other food outlets; over 81,000 domestic food facilities (e.g., warehouses; manufacturers; processors); and roughly 2.1 million farms.¹⁷² Similarly, according to the 2015 Healthcare and Public Health SSP, the array of entities that composed the Healthcare and Public Health Sector included entities that provide direct patient care (e.g., hospitals, urgent care clinics, doctor and dentist offices); medical research institutions; medical record system vendors; health insurance companies; local and State health departments;

¹⁶⁹ GCCs are formed as the government counterpart for each SCC to enable interagency and cross-jurisdictional coordination. The GCCs are comprised of representatives from across various levels of government (federal, state, local, or tribal), as appropriate to the operating landscape of each individual sector. See <https://www.cisa.gov/resources-tools/groups/government-coordinating-councils> (last visited Nov. 28, 2023).

¹⁷⁰ CISA’s website has a web page for each critical infrastructure sector, each of which includes a link to the sector’s respective SSP. These web pages are available at <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors> (last visited Nov. 28, 2023). The current versions of the SSPs are also collectively located at <https://www.cisa.gov/2015-sector-specific-plans> (last visited Nov. 28, 2023).

¹⁷¹ PPD-21 defines “critical infrastructure” as “having the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

¹⁷² DHS, *Food and Agriculture SSP* at 3 (2015), available at <https://www.cisa.gov/publication/nipp-ssp-food-ag-2015>.

cemeteries, crematoriums, morgues, and funeral homes; pharmaceutical and other medical supply manufacturers and distributors; medical laboratories; drug store chains; and blood banks.¹⁷³ As a third example, the 2015 Commercial Facilities SSP defines the Commercial Facilities Sector to include a mix of entities, such as the nation's 1.1 million malls, shopping centers, and other retail establishments; over 52,000 hotel-based properties; nearly 1,400 casinos and associated resorts; 1 million office buildings; 5.6 million multi-family rental buildings, and nearly 125,000 establishments designed for public assembly, such as stadiums, arenas, movie theaters, museums, zoos, libraries, and other performance venues.¹⁷⁴ CISA considered the variety of entities described in the sector profiles in the SSPs when determining the scope of the Applicability section.

CISA has determined it is appropriate to define entities within a critical infrastructure sector consistently with SSP sector profiles that were developed through a collaborative public-private partnership, as these sector profiles reflect a mutual understanding of what types of entities are in a critical infrastructure sector. This interpretation was supported by many commenters whose comments reflected the breadth of entities that are within a critical infrastructure sector.¹⁷⁵ Accordingly, CISA proposes to include an equivalently wide variety of types of entities within the scope of the CIRCIA regulatory description of "covered entity" to reflect the same diversity of entities that are in a critical infrastructure sector within the context of PPD-21, the NIPP, and each sector's SSP. This is also why CISA is not proposing to limit the scope of the

Applicability section to owners and operators of critical infrastructure.

A number of commenters have recommended that CISA limit the definition of covered entity to critical infrastructure or a subset thereof. CISA believes that interpretation is neither consistent with the authorization granted to CISA by Congress in CIRCIA, nor would it enable CISA to achieve the intended purposes of the regulation. To the first point, a plain language reading of CIRCIA's statutory definition of covered entity indicates that CISA has the authority to include within the scope of the regulation more than just entities that own or operate critical infrastructure. As demonstrated by the broad sector profiles in SSPs described above, CISA views the language used by Congress in CIRCIA bounding the scope of who could be a covered entity as simply "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21" as representative of a much broader set of entities than just owners and operators of critical infrastructure. Had Congress wanted to limit CISA's regulatory authority to critical infrastructure owners and operators, it could have easily done so, as PPD-21 includes a definition for the term "critical infrastructure" itself that could have been used for this purpose.¹⁷⁶

More importantly, such a narrowing scope of the term covered entity would severely hinder CISA's ability to achieve CIRCIA's regulatory purposes. As discussed earlier, CISA identified a number of purposes that the regulation is designed to facilitate. See Section III.C.i. Many of these purposes require a sufficient amount of data to achieve. These purposes include the identification of commonly exploited vulnerabilities and effective countermeasures; trend analysis and threat tracking, both generally and in relation to specific sectors, industries, or geographic regions; and the issuance of cybersecurity alerts and early warnings. See Section III.C.ii. Reporting from a broad range of entities is necessary to provide adequate visibility of the cyber landscape across critical infrastructure sectors, which CIRCIA is meant to facilitate. 6 U.S.C. 681a(a)(1). Furthermore, the products and analysis CISA is able to produce in support of these goals are likely to significantly improve in quality in proportion with increases in the amount of data

available to CISA to support its analytical activities.

To receive a sufficient number of reports to achieve these regulatory goals, CISA believes a broad interpretation of the term covered entity is essential. See Section III.C.ii. This is particularly necessary in light of the limitations Congress imposed on the term covered cyber incident which defines the types of incidents that must be reported under the proposed rule. As discussed later in this document, CISA interprets the Congressional language related to substantial cyber incident and, by proxy, the definition of covered cyber incident, to limit the types of incidents for which CISA can mandate reporting. As the number of CIRCIA Reports CISA will receive is a function of both whether an entity meets the description of a covered entity and whether the incident experienced meets the definition of covered cyber incident, narrowly interpreting both would severely restrict the number of incidents about which CISA receives information. Because CISA's discretion to define a covered cyber incident is more limited by CIRCIA itself, CISA believes it is important to scope covered entity, where it has greater discretion under CIRCIA, more broadly.

CISA is not, however, proposing to scope the term covered entity so broadly as to include virtually every entity within one of the critical infrastructure sectors within the description of covered entity. CISA believes that this is just the starting threshold at which Congress intended that CISA consider describing the contours of entities that should be included as covered entities. Rather, CISA's proposed Applicability section is designed to focus the reporting requirements primarily on entities that own or operate systems or assets considered critical infrastructure under the PPD-21 definition, while still requiring reporting from a small subset of entities that might not own or operate critical infrastructure but that could impact critical infrastructure to help ensure CISA receives an adequate number of reports overall, including reports of substantial cyber incidents from entities that are most likely to own or operate critical infrastructure. To achieve this, CISA is proposing a description for covered entity that would capture both entities of a sufficient size (based on number of employees or annual revenue) as well as smaller entities that meet specific sector-based criteria.

¹⁷³ DHS, *Healthcare and Public Health SSP at 5* (May 2016), available at <https://www.cisa.gov/resources-tools/resources/healthcare-and-public-health-sector-specific-plan-2015> (hereinafter "Healthcare and Public Health SSP").

¹⁷⁴ DHS, *Commercial Facilities SSP: An Annex to the NIPP 2013*, at 3 (2015), available at <https://www.cisa.gov/publication/nipp-ssp-commercial-facilities-2015>.

¹⁷⁵ See, e.g., Comments submitted by the National Retail Federation, CISA-2022-0010-0092-0001 (stating that food and beverage retailers and restaurants fall within the definitions of the Commercial Facilities Sector and/or the Food and Agriculture Sector); National Electrical Manufacturers Association, CISA-2022-0010-0026-0001 (noting in an example that shopping malls are part of the Commercial Facilities Sector); Rural Wireless Association, CISA-2022-0010-0093-0001 (acknowledging the entire communications sector may be included in the covered entity definition"); Center for Democracy and Technology, CISA-2022-0010-0068-0001 (citing the NIPP and Education Facilities SSP to show that all K-12 schools could be included as covered entities).

¹⁷⁶ See PPD-21, "Definitions" at 12, available at <https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and>.

ii. Determining if an Entity Is in a Critical Infrastructure Sector

As a threshold matter, to be a covered entity, an entity must be “an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21.” 6 U.S.C. 681. As noted above, PPD–21 does not actually include a definition for “critical infrastructure sector,” but rather provides a list of the sixteen critical infrastructure sectors and directed updates to the NIPP and the public-private partnership model (*i.e.*, SSPs).¹⁷⁷

CISA anticipates that the process for an entity to determine if it is within a critical infrastructure sector will usually be a relatively straightforward exercise. CISA has strong public-private partnerships with the critical infrastructure community, and will be leveraging these relationships as part of the outreach and education campaign that is required by CIRCIA to inform entities that are likely covered entities of the regulatory reporting requirements associated with this proposed rule.¹⁷⁸ CISA expects that entities will be able to obtain informational materials as part of this outreach and education campaign that will simplify the process of determining whether an entity is a covered entity. However, CISA has attempted to propose a population of entities in a critical infrastructure sector that would typically expect themselves to be included in a critical infrastructure sector, which will enable an entity to easily self-identify whether or not it is a covered entity. For example, entities engaged in or facilitating transportation, such as airplane or car manufacturers, airport and train station operators, and trucking companies, can readily self-identify as in the Transportation Services Sector. Similarly, entities engaged in the production, storage, and distribution of food, such as farms, food packagers and distributors, and grocery stores can readily self-identify as in the Food and Agriculture Sector. Banks, credit unions, credit card companies, registered broker-dealers, and other entities providing financial services can similarly self-identify as in the Financial Services Sector, while drinking water and wastewater treatment facilities can also readily identify as in the Water and Wastewater Systems Sector. Moreover, many of these same entities are members of the

SCC for their respective critical infrastructure sectors and on this basis would be able to accurately self-identify which critical infrastructure sector(s) they would fall within.¹⁷⁹

In some cases, however, it may be less obvious to an entity whether it falls into one or more of the critical infrastructure sectors. Examples include mine tailings and navigation locks (Dams Sector); nursing homes and cemeteries (Healthcare and Public Health Sector); and schools and elections infrastructure (Government Facilities Sector). The scope of types of entities that are considered part of a sector are described in the sector profiles in each sector’s SSP. As noted above in Section IV.B.i, SSPs are documents developed jointly by each sector’s SCC and GCC to help implement PPD–21 and the NIPP. The current versions of SSPs for all 16 sectors can be found on the CISA website at <https://www.cisa.gov/2015-sector-specific-plans>. The overwhelming majority of entities, though not all, are considered part of one or more critical infrastructure sectors. Illustrative examples of entities that generally are not considered part of one or more critical infrastructure sector include advertising firms, law firms, political parties, graphic design firms, think tanks, and public interest groups.

If an entity is unsure as to whether or not it is part of a critical infrastructure sector, CISA recommends the entity review the SSP for the sector or sectors that most closely align with the line of activities in which the entity is engaged. Once the final rule has issued, entities will also be able to reference informational materials that will be published as part of CISA’s outreach and education campaign. If after taking these steps, an entity still is unsure as to whether it is in a critical infrastructure sector, CISA recommends the entity contact CISA so that CISA can assist the entity in determining if it is in a critical infrastructure sector.

iii. Clear Description of the Types of Entities That Constitute Covered Entities Based on Statutory Factors

Section 681b(c)(1) of title 6, United States Code, requires CISA to include in the final rule “A clear description of the types of entities that constitute covered entities, based on—(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety; (B)

the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and (C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.”

The first part of this requirement is that CISA must provide “[a] clear description of the types of entities that constitute covered entities . . .” For the reasons described in this section, CISA believes that the criteria contained within the proposed Applicability section are easily understandable and clearly explain the types of entities that constitute covered entities. Accordingly, CISA believes that the Applicability section satisfies CIRCIA’s “clear description” requirement.

In developing this clear description of what is a covered entity, 6 U.S.C. 681b(c)(1) requires CISA to base this clear description on the three factors enumerated within that section. CISA understands 6 U.S.C. 681b(c)(1) not as imposing minimum requirements on what may be a covered entity, but rather simply as providing lenses through which CISA is to consider what entities it should seek to include in the description of covered entity. For example, CISA is to consider “the likelihood” an entity will be targeted, but 6 U.S.C. 681b(c)(1) does not require that entities be included in the description of covered entity only if they have a “high likelihood” or “very high likelihood” of being targeted.

Further, while 6 U.S.C. 681b(c)(1) uses the word “and,” CISA does not interpret 6 U.S.C. 681b(c)(1) as requiring that all three factors be relevant to each entity or category of entities included in the description of covered entity; rather, CISA reads the “and” as indicating that CISA must consider, as part of its process of determining the description of covered entity, all three factors. For example, an entity could be considered a covered entity if it maintains sensitive intellectual property, the compromise of which could cause significant national security or economic security consequences (factor A), even if unauthorized access to that information would not likely enable the disruption of reliable operation of critical infrastructure (factor C).

This interpretation is also consistent with the specifics of the 6 U.S.C. 681b(c)(1) factors themselves, which, collectively, address different aspects of risk. “Risk” is generally understood to be a measure of the extent to which an

¹⁷⁷ *Id.* at 10–11.

¹⁷⁸ See 6 U.S.C. 681b(e)(1); see also CISA’s Critical Infrastructure Partnership Advisory Council (CIPAC) website describing CISA’s partnership and forum with the critical infrastructure community at <https://www.cisa.gov/resources-tools/groups/critical-infrastructure-partnership-advisory-council-cipac> (last visited Nov. 28, 2023).

¹⁷⁹ See CISA’s Sector Coordinating Councils website for information on SCCs and membership for each sector’s SCC at <https://www.cisa.gov/resources-tools/groups/sector-coordinating-councils> (last visited Nov. 28, 2023).

entity is threatened by a potential circumstance or event, determined based on a function of (1) the consequences, or adverse impacts, that could arise if the circumstances or event occurs, and (2) the threat or vulnerabilities, or the likelihood of occurrence.¹⁸⁰ In the cybersecurity context specifically, risk is often understood to refer to those consequences and threats or vulnerabilities caused by or resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems. See 6 U.S.C. 650(7). This risk “equation” is often summarized as Risk = Consequence × Threat × Vulnerability. Viewed through this framing, CISA interprets the three factors listed in 6 U.S.C. 681b(c)(1) to each represent a different aspect of the risk equation: factor A (the consequence of disruption or compromise) addresses the “consequence” prong of the equation; factor B (the likelihood that such an entity may be targeted) addresses the “threat” prong; and factor C (the extent to which compromise of an entity could enable the disruption of reliable operation of critical infrastructure) speaks, albeit indirectly, to vulnerability, *i.e.*, the extent to which compromise of this entity could increase the vulnerability of critical infrastructure. Read through this lens, CISA understands the 6 U.S.C. 681b(c)(1) factors to be direction to CISA to consider specific aspects of the three prongs of cybersecurity risk—consequence, threat, and vulnerability—in assessing who should be deemed a covered entity. While the risk equation recognizes that an extremely low consequence can balance out a moderate threat to result in a generally low overall risk, a very high threat combined with even a moderate consequence, or a very high consequence combined with a moderately low threat can still lead to a moderate to high cybersecurity risk. With this understanding in mind, CISA interprets these factors not to limit the possible scope of covered entities to those entities that achieve high scores on each prong of the risk equation, but rather to use these factors to consider the various identified aspects of cybersecurity risk in determining which entities in a critical infrastructure sector should be covered entities. Moreover, if CISA were to interpret these three factors as requiring CISA only to deem

entities that meet all three as covered entities, this could result in CISA not receiving sufficient reporting across any given critical infrastructure sector to competently fulfill its statutory responsibilities under CIRCIA to aggregate and analyze information. As reflected in the discussion throughout this section, CISA considered all three factors enumerated in 6 U.S.C. 681b(c)(1) as it analyzed how to describe covered entity.

All three factors—*i.e.*, (A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety; (B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and (C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure—were particularly central to the determination of the sector-based criteria being proposed by CISA to augment the group of entities that would be considered covered entities under the first prong of the criteria contained in the Applicability section based on their size. These factors also drove CISA’s proposal to exclude entities in a critical infrastructure sector that fall below the size standards (unless they meet a sector-based criteria) while including entities in a critical infrastructure sector that are larger (even if not otherwise a covered entity based on the sector-based criteria).

While the discussion below is focused largely on the reasons why CISA is proposing to include entities in the description of covered entity based on the extent to which these factors apply in the context of covered cyber incident reporting requirements, the rationale generally holds true for ransom payment reporting requirements as well. CIRCIA provides one term—“covered entity”—to describe the scope of entities subject to both reporting requirements, and, consistent with this framing, CISA is proposing to apply the covered cyber incident reporting requirements and the ransom payment reporting requirements to the same universe of covered entities. This is also consistent with the three statutory factors described above, the current threat landscape related to ransomware attacks, and CISA’s responsibilities under CIRCIA. If a covered entity pays a ransom payment, it is likely that it has experienced a ransomware attack from which it has

not been able to recover quickly (*e.g.*, through the use of backup systems and data). To the extent a covered cyber incident against a particular entity would justify its inclusion in the description of covered entity due to the factors above (*e.g.*, the consequences that disruption to or compromise of such an entity could cause), so too would a ransomware attack from which an entity cannot quickly recover, as this would likely involve the very disruption or compromise envisioned by these factors. Further, in light of the rise of ransomware attacks as a proportion of cyber incidents,¹⁸¹ the rise of ransomware attacks targeting entities in critical infrastructure sectors specifically,¹⁸² and CISA’s statutory charge under CIRCIA to “coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments,” 6 U.S.C. 681a(a)(2), it is critical that CISA receive a sufficient number of Ransom Payment Reports from a breadth of entities in critical infrastructure sectors.

iv. Explanation of Specific Proposed Applicability Criteria

1. Size-Based Criterion

a. Overview

The first group of entities that CISA is proposing to include as covered entities are entities within a critical

¹⁸¹ See, *e.g.*, Verizon, *Data Breach Investigations Report at 7* (2022) (hereinafter, “Verizon 2022 DBIR”), available at <https://www.verizon.com/about/news/ransomware-threat-rises-verizon-2022-data-breach-investigations-report>.

¹⁸² See, *e.g.*, CISA, FBI, NSA, Australian Cyber Security Centre, and United Kingdom National Cyber Security Centre, *Joint Cybersecurity Advisory: 2021 Trends Show Increased Globalized Threat of Ransomware, AA22-040A* (Feb. 9, 2022), available at <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a> (“The [FBI], [CISA], and [NSA] observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, including the Defense Industrial Base, Emergency Services, Food and Agriculture, Government Facilities, and Information Technology Sectors. The Australian Cyber Security Centre (ACSC) observed continued ransomware targeting of Australian critical infrastructure entities, including in the Healthcare and Medical, Financial Services and Markets, Higher Education and Research, and Energy Sectors. The United Kingdom’s National Cyber Security Centre (NCSC–UK) recognizes ransomware as the biggest cyber threat facing the United Kingdom. Education is one of the top UK sectors targeted by ransomware actors, but the NCSC–UK has also seen attacks targeting businesses, charities, the legal profession, and public services in the Local Government and Health Sectors.”); FBI internet Crime Complaint Center, *internet Crime Report at 14* (2022), available at <https://www.ic3.gov/Home/AnnualReports> (noting that the internet Crime Complaint Center received 870 voluntary complaints that indicated organizations belonging to a critical infrastructure sector were victims of a ransomware attack, including at least 1 member of every critical infrastructure sector except Dams and Nuclear Reactors, Materials, and Waste Sectors).

¹⁸⁰ See, *e.g.*, NIST, *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards Publication 200 (March 2006) at 48, <https://doi.org/10.6028/NIST.FIPS.200> (last visited Mar. 12, 2024).

infrastructure sector that exceed the U.S. Small Business Administration's (SBA) small business size standard based on either number of employees or annual revenue, depending on the industry. For a number of reasons CISA believes a sensible approach is to require larger entities within a critical infrastructure sector to report cyber incidents while generally excluding smaller entities from those same reporting requirements.

In assessing whether to propose a size-based criterion as a basis for scoping which entities in a critical infrastructure sector should be considered covered entities, CISA took into consideration the three factors described in 6 U.S.C. 681b(c)(1). CISA believes that each of these factors support the inclusion of the very small percentage of businesses in the United States that exceed the small business size standards in the description of "covered entity."

The first factor Congress identified in 6 U.S.C. 681b(c)(1) is the consequences that disruption to or compromise of an entity could cause to national security, economic security, or public health and safety. While size is not alone indicative of criticality, larger entities' larger customer bases, market shares, number of employees, and other similar size-based characteristics mean that cyber incidents affecting them typically have greater potential to result in consequences impacting national security, economic security, or public health and safety than cyber incidents affecting smaller companies. For example, a successful cyber incident affecting a national drug store chain is much likelier to have significant national security, economic security, or public health and safety impacts than a similar incident affecting a "mom-and-pop" drug store. Similarly, there is a substantially higher likelihood of significant impacts resulting from a successful cyber incident affecting a large industrial food conglomerate, a multinational hotel chain, or a large hospital system than one affecting a small independent farm, a single-location bed and breakfast, or a small doctor's office, respectively. Countless other similar examples exist.

At least one other regulator has used the likelihood of greater consequences at larger facilities to justify imposing regulatory requirements based on company size. Specifically, the Food and Drug Administration's Mitigation Strategies to Protect Food Against Intentional Adulteration regulations at 21 CFR part 121 imposes less stringent regulatory requirements on small and very small businesses, stating that

larger, more well-known businesses "are likely to have larger batch sizes, [with attacks on them] potentially resulting in greater human morbidity and mortality. Further, an attack on a well-recognized, trusted brand is likely to result in greater loss of consumer confidence in the food supply and in the government's ability to ensure its safety and, consequently, cause greater economic disruption than a relatively unknown brand that is distributed regionally."¹⁸³ By requiring reporting from large entities, CISA is more likely to rapidly be informed about incidents impacting the largest number of people and creating the most significant national security, economic security, or public health and safety impacts.

The second factor Congress identified in 6 U.S.C. 681b(c)(1) for CISA to consider as part of scoping the description of covered entity is the likelihood that an entity may be targeted by a malicious cyber actor. Recent studies show that large entities disproportionately experience cyber incidents. Per the 2022 Verizon DBIR, from November 2021 through October 2022, entities with more than 1,000 employees experienced 23.5% of the cyber security incidents analyzed by Verizon for which the size of the organization was known,¹⁸⁴ despite entities with more than 1,000 employees accounting for less than 1% of U.S. businesses.¹⁸⁵ That percentage actually increased the following year, with the 2023 Verizon DBIR stating that entities with more than 1,000 employees experienced 41% of the cybersecurity incidents analyzed by Verizon for which the size of the organization was known during the relevant timeframe.¹⁸⁶ This is consistent with the belief that terrorist organizations and other bad actors frequently target larger, more well-known entities.¹⁸⁷ The desire to target

large entities has been noted specifically in regards to cyber incidents as well. For instance, per the 2024 Homeland Security Threat Assessment, based on trends from the first half of the year, the year 2023 was expected to be the second most profitable year ever for ransomware attackers due in part to "big game hunting," *i.e.*, the targeting of large organizations.¹⁸⁸

The third and final factor Congress identified in 6 U.S.C. 681b(c)(1) for CISA to consider as part of scoping the description of covered entity is the extent to which damage, disruption, or unauthorized access to such an entity will likely enable the disruption of the reliable operation of critical infrastructure. The majority of critical infrastructure is owned and operated by the private sector.¹⁸⁹ Although the percentage of critical infrastructure owned and operated by larger entities versus small businesses is unknown, given that the less than 1% of businesses in America that are not considered small businesses account for 56% of the United States' gross domestic product and employ nearly 54% of all private sector employees,¹⁹⁰ these entities are likely to own or

FR 78014, 78033 (Dec. 24, 2013) ("It is our assessment that [a desire to maximize public health harm and, to a lesser extent, economic disruption] are likely to drive terrorist organizations to target the product of relatively large facilities, especially those for which the brand is nationally or internationally recognizable. An attack on such a target would potentially provide the widescale consequences desired by a terrorist organization and the significant public attention that would accompany an attack on a recognizable brand.").

¹⁸⁸ Department of Homeland Security, 2024 *Homeland Security Threat Assessment* at 26 ("Ransomware attackers extorted at least \$449.1 million globally during the first half of 2023 and are expected to have their second most profitable year. This is due to the return of 'big game hunting'—the targeting of large organizations—as well as cyber criminals' continued attacks against smaller organizations."), available at <https://www.dhs.gov/publication/homeland-threat-assessment> (hereinafter, "2024 Homeland Security Threat Assessment"); see also Dmitry Dontov, *What Businesses are the Most Vulnerable to Cyberattacks*, *Forbes.com* (Jan. 19, 2021) ("[M]ature hacking groups like Evil Corp are going after large businesses, including Fortune 500 companies. Cybercriminals have their sights set on 'big fish' in various industries, as seen with attacks on Garmin, Blackbaud, Magellan Health and others."), available at <https://www.forbes.com/sites/theyec/2021/01/19/what-businesses-are-the-most-vulnerable-to-cyberattacks/?sh=331f38bf3534>.

¹⁸⁹ See, e.g., U.S. Government Accountability Office (GAO), GAO-22-104279: *CRITICAL INFRASTRUCTURE PROTECTION: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing* at 1 (Mar. 2022) ("The majority of critical infrastructure is owned and operated by the private sector."), available at <https://www.gao.gov/products/gao-22-104279>.

¹⁹⁰ U.S. Small Business Administration Office of Advocacy, *Frequently Asked Questions* (Mar. 2023), available at <https://advocacy.sba.gov/2023/03/07/frequently-asked-questions-about-small-business-2023/> (last visited Nov. 28, 2023).

¹⁸³ 78 FR 78033 (Dec. 24, 2013).

¹⁸⁴ *Verizon 2022 DBIR*, *supra* note 181, at 50 (for the 2,701 incidents analyzed by Verizon that occurred between November 1, 2021 and October 31, 2022 and for which Verizon knew the impacted organization's size, 636 had more than 1,000 employees).

¹⁸⁵ According to the U.S. Census Bureau, in 2021, only 8,365 out of 8,148,606 (or .1%) of companies with one or more employees had 1,000 or more employees. See U.S. Census Bureau, 2021 County Business Patterns, available at <https://www.census.gov/programs-surveys/cbp/data.html>.

¹⁸⁶ Verizon, *Data Breach Investigations Report* at 50 (2023) (for the 1,183 incidents analyzed by Verizon that occurred between November 1, 2021 and October 31, 2022 and for which Verizon knew the impacted organization's size, 489 had more than 1,000 employees) (hereinafter, "Verizon 2023 DBIR"), available at <https://www.verizon.com/business/resources/reports/dbir/2023/master-guide/>.

¹⁸⁷ See, e.g., *Focused Mitigation Strategies To Protect Food Against Intentional Adulteration*, 78

operate a disproportionate percentage of the nation's critical infrastructure. Moreover, in light of the interconnectedness of the world today, incidents at entities in critical infrastructure sectors that are not themselves owners and operators of critical infrastructure can have cascading effects that end up impacting critical infrastructure. Based on this, CISA believes that substantial cyber incidents (which, as described below, are the types of incidents that covered entities are required to report) at larger entities routinely will have a high likelihood of disrupting the reliable operation of critical infrastructure.

In addition to the rationales provided based on CISA's consideration of the 6 U.S.C. 681b(c)(1) factors, CISA believes there are additional reasons justifying the proposed sized-based criteria to scope covered entity. For instance, larger entities also are likely to have more mature cybersecurity capabilities or be better situated to bring in outside experts to assist during an incident.¹⁹¹ These capabilities make larger entities more likely to identify early signs of compromise than smaller entities. By including large entities in the description of covered entity, the likelihood that an incident is noticed and reported is increased, while the timeframe between initiation of an incident and its reporting is likely to be decreased.

For similar reasons, CISA believes larger entities also frequently will be better situated to simultaneously report and respond to or mitigate an incident, which is a situation many, if not most, reporting entities will be faced with given the statutorily mandated 72-hour reporting requirement for Covered Cyber Incident Reports and 24-hour reporting requirement for Ransom Payment Reports. Finally, larger entities generally will be better situated to absorb costs associated with reporting, even if per-report costs are relatively minimal, which CISA believes they will be. Given this, to the extent that CISA is offering regulatory relief to a portion of the community that Congress included in the statutory definition of covered entity

(the regulatory relief being not including certain entities as covered entities in the proposed Applicability section in § 226.2), CISA believes that relief should be provided to smaller businesses that may be less capable of absorbing costs associated with incident reporting to the extent they do not fit within the sector-based criteria described below. Such an approach is also consistent with the goals of the Small Business Regulatory Enforcement Fairness Act, which Congress enacted in large part to ensure departments and agencies explore options for reducing any significant economic impact on small businesses that, based on their more limited resources, may have greater difficulty understanding and complying with regulations.¹⁹²

CISA believes that this proposed approach has ancillary benefits as well. First, employee- and revenue-based criteria have a long history of use for other purposes, including regulatory purposes.¹⁹³ CISA additionally believes that most entities should be able to relatively easily determine if they meet the size-based requirements for inclusion as a covered entity. The desire for definitional clarity was a common refrain raised by stakeholders during CIRCIA listening sessions and in comments submitted in response to the RFI. CISA believes this aspect of the Applicability Section (as well as the Applicability section as a whole) achieves that clarity. Second, while CISA believes the costs incurred by an individual entity associated with reporting an incident under the proposed regulation are relatively low, by removing small businesses from the description of covered entity unless they meet a specific sector-based reason for inclusion, CISA will significantly lower the aggregated costs associated with this regulatory program.

In response to the CIRCIA RFI, several commenters advocated for CISA to use a size-based threshold that would allow CISA to broadly capture entities above a certain size. Multiple commenters recommended the definition of covered entity include all entities with 50 or more employees,¹⁹⁴ with some also

recommending it include entities with more than 1,000 customers or \$5 million in revenue.¹⁹⁵ One commenter suggested exempting from coverage entities that meet the SBA definition of a small business for certain North American Industry Classification System (NAICS) codes.¹⁹⁶

Contrarily, a number of stakeholders recommended against using a size threshold for identifying covered entities because the size of an entity does not necessarily equate to criticality.¹⁹⁷ These stakeholders argued that using a size threshold would: (a) cause CISA to miss reports from entities that own, or provide products or services to, critical infrastructure that fell below the chosen threshold; and (b) require reporting of incidents from entities that do not own or operate systems or assets that are critical infrastructure, which a number of the commenters asserted is not in line with the purposes of the regulation. While CISA agrees with commenters that the size of an entity does not necessarily equate to that entity's criticality, it does not believe the two outcomes the commenters suggest will occur or have the negative impact suggested based on how CISA has proposed to scope the description of covered entity.

Regarding the first concern, that using a size-based standard would cause CISA to miss reports from critical infrastructure entities that fall below the size standard, CISA would agree with this if a size-based standard was the only way in which an entity could become a covered entity. To address this

CISA-2022-0010-0019, and SolarWinds, CISA-2022-0010-0027.

¹⁹⁵ See Comments submitted by the Cyber Threat Alliance, CISA-2022-0010-0019; SolarWinds, CISA-2022-0010-0027.

¹⁹⁶ See Comment submitted by the National Grain and Feed Association, CISA-2022-0010-0104.

¹⁹⁷ See, e.g., Comments submitted by the Information Technology-ISAC, CISA-2022-0010-0048 ("Focusing on the incident's impact on critical infrastructure might also provide a path to defining the term 'covered entity.' For example, if the goal of the program is to manage risks and disruptions to critical infrastructure, CISA could define 'covered entities' based on the products or services companies provide to critical infrastructure. In this way, a covered entity is not determined by its size, but by the criticality of the products or services it provides to other critical infrastructure."); (ISC)2, CISA-2022-0010-0112 ("Each of the 16 critical infrastructure sectors has varying risk profiles which should be considered when considering this definition. We suggest basing the definition on the nature of those services and the effect it could have on customers instead of employees and revenue."); NCTA—The Internet & Television Association, CISA-2022-0010-0102 ("Covered entity eligibility criteria that are size- and sector-neutral are critical because the online ecosystem consists of a broad range of interdependent entities, including communications networks, cloud services, CDN providers, software and security vendors, and e-commerce platforms and applications.").

¹⁹¹ *Verizon 2023 DBIR*, *supra* note 186, at 65 ("In certain prior reports, we have compared and contrasted small and medium businesses (SMBs) against large organizations to determine whether the attack surface differed significantly between them. Increasingly, both SMBs and large companies are using similar services and infrastructure, and that means that their attack surfaces share more in common than ever before. This has led to a convergence of attack profiles regardless of the size of the organization. However, what is very different is the ability of organizations to respond to threats due to the number of resources they can deploy in the event that they are attacked.").

¹⁹² See 5 U.S.C. 601 *et seq.*

¹⁹³ See, e.g., 7 CFR 205.236(d)(1) (provides certain exceptions to small businesses as determined by 13 CFR part 121 for requirements applicable to foods labeled as organic); 40 CFR 86.1801-12(j) (exempts small businesses meeting the SBA size standards from certain vehicle greenhouse gas emission standards); 40 CFR part 1033 (provides different locomotive emissions standards for "small railroads" which, among other things, must meet the SBA size standards to qualify).

¹⁹⁴ See e.g., Comments submitted by the Computing Technology Industry Association, CISA-2022-0010-0122, Cyber Threat Alliance,

concern and ensure that most entities that own or operate critical infrastructure are included within the covered entity description regardless of size, CISA has included additional sector-based criteria in the Applicability section which, if met by an entity in a critical infrastructure sector, would make that entity a covered entity, even if the entity's size is below the applicable size standard. Many of the sector-based criteria are specifically designed to target entities that own or operate critical infrastructure, and these criteria are independent of the size standard for determining applicability of the proposed regulations. In other words, an entity in a critical infrastructure sector is a covered entity if it meets any of the criteria included in the Applicability section, be it the size-based standard or one of the sector-based criteria. As noted earlier, an entity in a critical infrastructure sector does not have to meet both the size-based standard and one of the sector-based criteria for inclusion as a covered entity.

As to the second concern, that size-based thresholds will result in reporting of incidents from entities that do not own or operate systems or assets that constitute critical infrastructure and that those reports would not advance the purposes of the regulation, CISA agrees with the first part of the comment, but not the latter. CISA agrees that size is not always indicative of criticality, and thus, including all entities of a certain size that are within a critical infrastructure sector as covered entities will result in CISA receiving some reporting from entities that are in critical infrastructure sectors, but do not own or operate systems or assets that constitute critical infrastructure. CISA, however, disagrees that CISA requiring reporting from those entities that do not own or operate critical infrastructure would not support the purposes of this regulation. Incidents that occur at entities in critical infrastructure sectors reveal valuable information on TTPs and trends that can be used to help better protect other entities in those specific sectors and others, regardless of whether the reporting entities own or operate systems or assets that constitute critical infrastructure. If CISA were to require reporting on only significant incidents from entities that own or operate critical infrastructure, CISA's ability to identify adversary trends and campaigns, identify vulnerabilities that are being exploited, and issue early warnings would be significantly more limited. It is much more in line with the purpose of the regulation for CISA to learn about new or novel vulnerabilities,

trends, or tactics sooner and be able to share early warnings before additional entities within a critical infrastructure sector, whether or not they own or operate critical infrastructure, can fall victim to them.

Additionally, in light of the interconnectedness of the world today, incidents at entities in a critical infrastructure sector, even if that the entity does not own or operate critical infrastructure, can have unexpected, cascading effects that end up impacting critical infrastructure.¹⁹⁸ Requiring reporting from entities in critical infrastructure sectors, whether or not they own or operate systems or assets that are critical infrastructure, can enable response and mitigation activities that may help prevent incidents from causing cascading impacts to critical infrastructure or hamper the delivery of NCFs.

b. Proposed Size-Based Criterion

CISA is proposing that the description of covered entity include any entity in a critical infrastructure sector that exceeds the small business size standard specified by the applicable North American Industry Classification System Code in the SBA Size Standards, which are codified in 13 CFR part 121. These standards "define whether a business is small and, thus, eligible for Government programs and preferences reserved for 'small business' concerns."¹⁹⁹ While designed in large part for determining eligibility to participate in certain Federal government contracts, procurements, grants, and other similar purposes, the Small Business Size Regulations indicate that the SBA Size Standards are for general use by Federal departments and agencies promulgating regulations that include size criteria.²⁰⁰ If a Federal department or agency wants to use different size criteria, it is required to consult with the SBA in writing during the rulemaking process and explain why the SBA's existing size standards would not satisfy program requirements.²⁰¹

SBA Size Standards vary by industry (as designated by NAICS²⁰² code) and

¹⁹⁸ See, e.g., CISA, *A Guide to Critical Infrastructure Security and Resilience* at 6 (Nov. 2019) ("Connections and interdependencies between infrastructure elements and sectors means that damage, disruption, or destruction to one infrastructure element can cause cascading effects, impacting continued operation of another."), available at <https://www.cisa.gov/resources-tools/resources/guide-critical-infrastructure-security-and-resilience> (hereinafter "*Guide to Critical Infrastructure Security and Resilience*").

¹⁹⁹ See 13 CFR 121.101(a).

²⁰⁰ See 13 CFR 121.903(a).

²⁰¹ *Id.*

²⁰² NAICS is the standard used by Federal statistical departments and agencies in classifying

are generally based on the number of employees or the amount of annual receipts (*i.e.*, annual revenue) the business has. SBA reviews and updates the Size Standards every five years via rulemaking. The current SBA Size Standards are contained in the SBA's Table of Small Business Size Standards, effective January 1, 2022, which can be found at both 13 CFR 121.201 and <https://www.sba.gov/document/supportable-size-standards>. Currently, the threshold for those industries where small business status is determined by number of employees is between 100 and 1,500 employees depending on the industry. The threshold for those industries where small business status is determined by annual revenue is between \$2.25 million and \$47 million depending on the industry. It is estimated that, as of 2022, there are more than 32 million small businesses in the United States, and that small businesses comprise 99.9% of all American businesses.²⁰³

In establishing its Size Standards, the SBA considers economic characteristics comprising the structure of an industry, such as degree of competition, average firm size, and distribution of firms by size, as well as competition from other industries, growth trends, historical activity within an industry, and unique factors occurring in the industry which may distinguish small firms from other firms.²⁰⁴ As the establishment of the SBA Size Standards is done via regulation, the public is afforded the opportunity to review and provide comments on any proposed modifications to existing SBA Size Standards before they go into effect. In light of the comprehensive and transparent process through which the SBA establishes its Size Standards, and the successful use of these standards as size-based thresholds for various Federal programs, CISA believes the SBA Size Standards are well-suited for use as the size-based threshold aspect of the CIRCIA Applicability section.

In determining the approach to propose for the covered entity description's size threshold, CISA also considered working with the SBA to

business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy. Additional information on NAICS, to include a listing of current NAICS codes, can be found at <https://www.census.gov/naics/> (last visited Nov. 28, 2023).

²⁰³ See, e.g., Kelly Main, *Small Business Statistics of 2023*, *Forbes* (Dec. 7, 2022), available at <https://www.forbes.com/advisor/business/small-business-statistics/>; U.S. Chamber of Commerce, *Small Business Statistics*, <https://www.chamberofcommerce.org/small-business-statistics/> (last visited Nov. 28, 2023).

²⁰⁴ 13 CFR 121.102(a).

establish a size standard for entities in critical infrastructure sectors tailored to the CIRCIA program. In exploring this option, CISA assessed whether a clear justification existed for using higher or lower thresholds than those established by the SBA Size Standards. CISA also considered whether a single threshold for all entities, rather than industry-specific thresholds, might be warranted. Ultimately, CISA, based in part on conversations with SBA, did not believe sufficient justification existed to deviate from the existing SBA Size Standards in any of these manners.

The first alternative CISA considered was the use of higher thresholds than those established in the SBA Size Standards. By raising the threshold—*i.e.*, increasing the minimum number of employees or amount of annual receipts an entity has to have before qualifying as a covered entity—CISA would be further reducing the number of entities that would qualify as covered entities. Considering the significant number of entities for whom using the SBA Size Standards as the threshold would provide regulatory relief, CISA believes that there is no need to generally exclude additional entities. Conversely, for the reasons discussed earlier supporting the need for broad collection of reports, CISA is concerned that any further reduction in the number of covered entities could make it difficult for CISA to achieve the goals of the regulation. See Section III.C.ii.

The second alternative CISA considered was the use of lower thresholds than those established in the SBA Size Standards. By lowering the threshold—*i.e.*, decreasing the minimum number of employees or amount of annual receipts an entity has to have before qualifying as a covered entity—CISA would be expanding the number of entities that would qualify as covered entities under this threshold. For the reasons discussed above, CISA believes it does not need to collect reports from the entire possible universe of covered entities allowed under the statutory language and that it is prudent to provide regulatory relief to smaller entities where possible. To the extent that some categories of entities from whom CISA believes reporting is important fall below the size threshold, CISA will be able to include those entities in the description of covered entity using the proposed sector-based criteria.

Finally, CISA explored whether there might be some benefit to using a single size-based threshold (or two—*i.e.*, one each for number of employees and annual receipts), as opposed to the SBA Size Standards approach that

establishes bespoke thresholds for more than 1,000 individual industries based on their NAICS codes. CISA does believe that using a single size-based threshold (or two) that would be consistent across all industries would be a simpler, clearer approach; however, the SBA has consistently determined that using size thresholds tailored by industry is important to respecting relevant and significant distinctions across different industries. Not only does the SBA use that approach in its own Size Standards, the Small Business Size Regulations require the SBA Administrator to ensure that any size standard approved by the SBA for use by other Federal regulators under the 13 CFR 121.903 process “varies from industry to industry to the extent necessary to reflect the differing characteristics of the various industries, and consider other relevant factors.”²⁰⁵ In light of this, CISA believes the best approach would be to use the SBA Size Standards as the basis for the CIRCIA size threshold.

c. How To Determine Whether an Entity Meets the Size Threshold

To determine if an entity in a critical infrastructure sector meets the proposed size threshold, an entity will need to determine which NAICS code should be applied to the entity and whether the entity meets the applicable employee-based or annual receipts-based threshold. The SBA’s Small Business Size Regulations provide requirements for how to determine if an entity qualifies as a small business under SBA regulations.²⁰⁶ This includes, among other things, requirements for determining which NAICS code applies to a given entity (13 CFR 121.101), how to calculate number of employees (13 CFR 121.106), and how to calculate annual receipts (*i.e.*, annual revenue) (13 CFR 121.104). CISA does not see any reason to deviate from this well-established approach to determining an entity’s size and thus is proposing to use the instructions found in the SBA’s Small Business Size Regulations as the methodology to be used to determine if an entity meets the CIRCIA covered entity size threshold. Accordingly, CISA is proposing that when an entity is determining whether it meets the size threshold provided in the Applicability section, the entity should follow the instructions contained in the Small Business Size Regulations, 13 CFR part 121, or any successor thereto.

CISA recognizes that entity size and other characteristics can be dynamic,

and whether an entity meets the size-based threshold or other criteria for being a covered entity may vary depending on when the entity assesses if they meet the criteria set forth in § 226.2. See discussion on reporting requirements in Section IV.C.i in this document for more information.

2. Sector-Based Criteria

CISA is also proposing to include as part of the description of covered entity in the Applicability section a series of criteria that are based on characteristics typically associated with entities in one or more specific critical infrastructure sectors or subsectors. Specifically, CISA is proposing to include in the scope of covered entity any entity that meets one or more of a set of specified sector-based criteria, each of which is described below. These criteria apply regardless of the specific critical infrastructure sector of which the entity considers itself to be part.

CISA is proposing these additional, sector-based criteria for a variety of reasons. First, as noted in the discussion regarding the size-based criterion, an entity’s size does not necessarily reflect its criticality. Some entities in a critical infrastructure sector that fall below the proposed size-based thresholds own or operate systems or assets that would be likely to meet the definition of critical infrastructure set forth by 42 U.S.C. 5195c(e). One of the main purposes of this regulatory program authorized by CIRCIA is to enhance the security and resiliency of critical infrastructure, and therefore receiving Covered Cyber Incident Reports and Ransom Payment Reports from as many entities that own or operate critical infrastructure as possible is imperative to meet this directive.

Another designated purpose of the CIRCIA regulation is for CISA to develop and share information on cybersecurity trends and threats. CISA believes that in addition to cross-sector cybersecurity threat and trend analysis, there is great value to being able to produce sector-specific threat and trend analysis. To achieve the latter, it is essential for the Federal government to have sufficient reporting from each critical infrastructure sector. For some sectors or subsectors, such as the Water and Wastewater Systems Sector, there currently is little or no required reporting of cyber incidents to the Federal government, making it very difficult for CISA or other Federal partners to provide reliable, incident-based, sector-specific trend and threat analysis. CISA believes the proposed sector-based criteria will help ensure the Federal government has sufficient

²⁰⁵ 13 CFR 121.903(b).

²⁰⁶ See 13 CFR 121.103–121.107.

reporting within each sector to support this type of analysis.

Third, consistent with the factors in 6 U.S.C. 681b(c)(1), CISA believes that broader coverage may be warranted for those sectors, subsectors, or industries that have historically been inordinately targeted by malicious cyber actors, including by foreign countries, or for which there is a greater likelihood of significant national security, economic security, or public health and safety consequences or disruption to the reliable operation of critical infrastructure. By ensuring CISA receives CIRCIA Reports from entities, regardless of size, in these more frequently or likely targeted sectors, subsectors, or industries, and entities against whom a covered cyber incident is more likely to result in significant consequences or disruptions to critical infrastructure, CISA and its partners will be better situated to identify new TTPs, campaigns, and vulnerabilities and share early warnings and prevention measures to help entities in those communities address the potential heightened threat for them of cyber incidents.

Based on the above rationales, CISA is proposing sector-based criteria for entities operating in each of the critical infrastructure sectors listed below. During the development of these proposed criteria, CISA engaged each of the SRMAs to consult on potential criteria for their respective sector, as well as other Federal agencies with cybersecurity-related regulatory authorities focused on specific sectors. CISA also considered the inputs received from the public through both the CIRCIA listening sessions and in response to the CIRCIA RFI.

For the proposed sector-based criteria, CISA proposes to cover entities that own or operate certain types of facilities or entities that perform certain functions as covered entities. For example, the Chemical Sector sector-based criteria proposes capturing within the description of covered entity any entity that owns or operates a CFATS-covered chemical facility, and the Healthcare and Public Health sector-based criteria would include, among others, entities that manufacture any Class II or III medical device. See Section IV.B.iv.2.a and i in this document. While these criteria are focused on certain facility types or functions as the basis of determining whether an entity is a covered entity, CISA is proposing that the entire entity (*e.g.*, corporation, organization), and not the individual facility or function, is the covered entity. Thus, for example, if an entity owns 20 chemical distribution facilities,

only five of which are CFATS-regulated facilities, the entire entity is the covered entity, and not simply the five CFATS-regulated facilities. Accordingly, if that entity experiences a substantial cyber incident or makes a ransom payment, the entity would need to report that incident or payment to CISA regardless of whether the underlying incident impacted any of the five CFATS-regulated facilities. Similarly, if an entity manufactures Class II or III medical devices, in addition to other functions that do not meet one of the sector-based criteria, the entire entity is the covered entity, and any substantial cyber incident experienced by any part of the entity would need to be reported, regardless of whether the underlying incident impacted the manufacturing of Class II or III medical devices. CISA believes this is consistent with CIRCIA's entity-based approach, and will ensure that adequate reporting is provided to CISA to perform sector-specific cybersecurity threat and trend analysis, which might not be possible if reporting was limited only to incidents that actually impact the specific facilities or functions identified in the sector-based criteria. Considering the entire entity (*e.g.*, corporation, organization), and not an individual facility or function, as the covered entity will also avoid delays in reporting that could be caused if entities had to wait to specifically determine whether particular facilities or functions were impacted by a substantial cyber incident.

a. Chemical Sector

CISA is proposing to include in the description of covered entity any entity in a critical infrastructure sector that owns or operates a covered chemical facility subject to the Chemical Facility Anti-Terrorism Standards.²⁰⁷ CISA proposes including this criterion to ensure that entities that own or operate a covered chemical facility that presents a high risk of significant adverse consequences for human life or health, national security, and/or critical economic assets if subjected to terrorist attack, compromise, infiltration, or

²⁰⁷ See 6 CFR part 27. CISA is aware that, at the time of publication of this NPRM, Congress has allowed statutory authority for the CFATS program to expire. CISA believes that by the time the CIRCIA final rule is issued, CFATS will be reauthorized by Congress. Should CFATS not be reauthorized by the time the CIRCIA final rule is ready for publication, CISA proposes to replace the proposed CFATS-based Chemical Sector criterion in this NPRM with an alternate Chemical Sector criterion focused on owners and operators of facilities regulated by the Environmental Protection Agency (EPA) under its Risk Management Program (RMP) regulations. That alternative is discussed at the end of this subsection.

exploitation are required to report substantial cyber incidents to CISA.

Under CFATS, any facility that possesses a threshold quantity of one of more than 300 chemicals of interest must provide information to CISA to enable CISA to conduct a risk assessment of the facility. See 6 CFR 27.200. If CISA determines that the facility is high-risk based on this assessment, the facility is required to develop and implement a site security plan, which must include appropriate cybersecurity measures. See 6 CFR 27.210(a)(3). These facilities are referred to under the CFATS regulations as covered chemical facilities.

Consideration of the three factors enumerated in 6 U.S.C. 681b(c)(1) also supports the inclusion of entities that own or operate CFATS covered chemical facilities within the description of covered entity. To determine if a chemical facility is high-risk and thus subject to CFATS, CISA conducts a risk assessment on the facility that considers the potential consequences of a successful attack on the facility, the level of threat facing the facility, and the vulnerability of the facility to an attack.²⁰⁸ Only chemical facilities that have the potential to cause significant consequences to public health and safety if compromised by terrorism (*i.e.*, the first factor identified in 6 U.S.C. 681b(c)(1), which relates to consequence) and face a high potential threat (*i.e.*, the second factor identified in 6 U.S.C. 681b(c)(1), which relates to likelihood of threat) will meet the criteria to be designated a CFATS covered chemical facility. As such, CISA believes that the first two factors enumerated in 6 U.S.C. 681b(c)(1) support the inclusion of entities that own or operate CFATS covered chemical facilities within the description of covered entity. The third factor enumerated in 6 U.S.C. 681b(c)(1), which refers to the extent to which damage, disruption, or unauthorized access to such an entity will likely enable the disruption of the reliable operation of critical infrastructure, similarly supports inclusion of these entities, as most, if not all, CFATS covered chemical facilities would meet the definition of critical infrastructure based on the potential national security or public health and safety consequences associated with a successful attack on the facility.

²⁰⁸ See CISA, *CFATS Tiering Methodology Fact Sheet*, available at <https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/cfats-tiering-methodology> (last visited Oct. 15, 2023).

As noted in the previous section of this document, while CFATS security requirements apply only to the covered chemical facilities themselves, CISA is proposing in this NPRM that the CIRCIA cyber incident reporting requirements apply to the entire corporate entity that owns or operates the CFATS-covered chemical facility and are not limited to substantial cyber incidents that impact a CFATS-covered chemical facility. CISA believes this is consistent with CIRCIA's entity-based approach and will ensure that adequate reporting is provided to CISA to perform chemical sector cyber threat and trend analysis, which might not be possible if reporting were limited only to incidents that actually impact CFATS-covered chemical facilities.

Because CFATS currently requires covered chemical facilities to report certain incidents, including potential cyber incidents, to CISA, CISA recognizes that this proposed criteria likely will result in two different legal obligations for certain entities to report cyber incidents to CISA under certain circumstances, depending on whether it is reporting a covered cyber incident or not. To avoid the same entity having to report the same incident to CISA twice, CISA is proposing that submission of a cyber incident report to CISA under either one of these authorities will satisfy the incident reporting obligations for both regulations for the incident, assuming the single submission includes all the information required to comply with both CFATS and CIRCIA, independently. However, if a covered entity reports an incident to CISA per CFATS requirements and intends for this report to also meet its reporting obligations under CIRCIA, it would need to indicate that intent in the submission. Otherwise, a separate CIRCIA Report would need to be filed to meet the entity's reporting obligations.

Finally, CISA also is aware that a number of high-risk chemical facilities may not be subject to CFATS under one of the statutory exemptions in the legislation authorizing CFATS. Specifically, CFATS does not apply to facilities regulated under MTTSA; public water systems, as that term is defined in 42 U.S.C. 300f; Treatment Works, as that term is defined in 33 U.S.C. 1292; or facilities subject to regulation by the NRC. 6 CFR 27.110(b). As a result, many entities that own high-risk chemical facilities would not be required to report cyber incidents to CISA either under CFATS or under this proposed sector-based criteria. CISA is proposing to require each of these categories of entities to file a CIRCIA Report under

various other sector-based criteria, however, so CISA ultimately is proposing that all entities that own or operate a high-risk chemical facility must report covered cyber incidents and ransom payments under one of the sector-based criteria.

As noted in an earlier footnote, CISA is aware that, at the time of publication of this NPRM, Congress allowed the statutory authority for CFATS to expire. CISA believes that by the time the CIRCIA final rule is issued, CFATS will be reauthorized, but also recognizes that it is prudent to include for public consideration a proposed alternative Chemical Sector sector-based criterion should CFATS not be reauthorized. Accordingly, CISA proposes that if CFATS is not reauthorized by the time the CIRCIA final rule is ready for publication, CISA instead would replace the CFATS-based Chemical Sector criterion with a Chemical Sector sector-based criterion that description identifies owners and operators of facilities subject to the EPA RMP rule as covered entities.

The EPA RMP rule, which is authorized by Section 112(r) of the Clean Air Act,²⁰⁹ requires facilities that use certain extremely hazardous substances to develop a risk management plan for chemical accident prevention purposes.²¹⁰ For similar reasons as those provided above in relation to the proposed CFATS-focused Chemical Sector sector-based criterion, a consideration of the 6 U.S.C. 681b(c)(1) factors would also support the inclusion of entities that own or operate facilities that are required to comply with EPA RMP requirements in the description of covered entity. According to the EPA, such chemical accidents that occur at such facilities can pose significant consequence and potential threat to national security and public health and safety because “[f]acilities subject to the RMP regulation pose significant risks to the public and the environment. These risks stem from potential accidental chemical releases that can cause fires, explosions, and harmful vapor clouds.”²¹¹ Furthermore, according to the U.S. GAO, “[t]housands of high-risk chemical facilities may be subject to the

²⁰⁹ See 40 CFR part 68.

²¹⁰ See EPA, *Risk Management Program (RMP) Rule Overview*, <https://www.epa.gov/rmp/risk-management-program-rmp-rule-overview> (last visited Nov. 28, 2023).

²¹¹ Reconsideration of the 2017 Amendments to the Accidental Release Prevention Requirements: Risk Management Programs Under the Clean Air Act, Section 112(r)(7), *Regulatory Impact Analysis* at 76 (Nov. 18, 2019), available at <https://www.regulations.gov/document/EPA-HQ-OEM-2015-0725-2089>.

risk posed by cyber threat adversaries—terrorists, criminals, or nations. These adversaries could potentially manipulate facilities' information and control systems to release or steal hazardous chemicals and inflict mass casualties to surrounding populations.”²¹² Moreover, as part of the development of the CFATS program's regulations, DHS drew from information and sources available through EPA RMP, including the list of substances used by EPA RMP to regulate facilities, due to the overlapping safety and security concerns associated with many chemicals.²¹³

For the reasons described above, CISA believes entities owning facilities subject to EPA RMP would be a satisfactory alternate criterion for ensuring CISA receives reporting under CIRCIA from entities within the Chemical Sector, and is supported by the three factors in 6 U.S.C. 681b(c)(1); however, CISA believes the CFATS-targeted criterion would be a better criterion for the Chemical Sector, if permissible, for a few reasons. First, regulation under the EPA RMP rule is limited to facilities that only present toxic or flammable release concerns because they impact public health and safety, whereas CFATS regulates facilities that are high risk due to other chemical security related concerns. Additional security concerns posed by CFATS includes coverage of chemicals that pose risks related to theft or diversion of explosives or weapons of mass effect, in addition to toxic and flammable release hazards. Second, whereas EPA RMP determines coverage primarily based on the potential consequences of a chemical release, CFATS additionally is required to take into account threat when determining if a facility is a CFATS covered chemical facility. Finally, because CFATS imposes cyber incident reporting requirements, using CFATS as a basis for the CIRCIA cyber incident reporting requirements coverage promotes harmonization of Federal cyber incident reporting regulations by aligning reporting requirements for the same population of entities. For these reasons, CISA is proposing to include a criterion capturing entities that own or operate facilities regulated under EPA RMP within the description of covered entity only if CFATS is not authorized at the time of the issuance of the CIRCIA final rule.

²¹² U.S. GAO, *GAO-20-453: CRITICAL INFRASTRUCTURE PROTECTION: Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities* (May 2020), available at <https://www.gao.gov/products/gao-20-453>.

²¹³ See 72 FR 17688 (Apr. 9, 2007).

CISA is interested in receiving comments on these two alternatives, to include:

10. The decision to solely use the CFATS-based criterion if CFATS is in effect at the time of the issuance of the CIRCIA final rule.

11. Other possible alternatives that CISA should consider as a sector-based criterion for the Chemical Sector if CFATS is not reauthorized by Congress.

b. Communications Sector

CISA is proposing to include in the description of covered entity any entity that provides communications services by wire or radio communications, as defined in 47 U.S.C. 153(40), 153(59), to the public, business, or government. This criterion would also require reporting from both one-way communications service providers (e.g., radio and television broadcasters, cable television and satellite operators) and two-way communications service providers (e.g., telecommunications carriers; submarine cable licensees; fixed and mobile wireless service providers; VoIP providers; internet service providers), irrespective of whether they are subject to FCC regulatory reporting or other FCC requirements.

Consideration of the factors enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of both one-way and two-way communications service providers within the description of covered entity. First, the disruption or compromise of either one-way or two-way communications systems could significantly impact national security, economic security, and public health and safety. As noted in the 2015 Communications SSP, “[v]irtually every element of modern life is now dependent on cyber infrastructure. As a result, our Nation’s economic and national security relies on the security of the assets and operations of critical communications infrastructure.”²¹⁴ Executive Order 13618—Assignment of National Security and Emergency Preparedness Communications Functions reinforces the importance of these entities to national security, stating that “[t]he Federal Government must have the ability to communicate at all times and under all circumstances to carry out its most critical and time sensitive missions. . . . Such communications must be possible under all circumstances to ensure national security, effectively manage

emergencies, and improve national resilience.”²¹⁵

One-way communications services providers are the primary providers of information, including emergency alerts, to the public. Therefore, a covered cyber incident affecting one-way communications service providers has the potential to significantly jeopardize public health and national security by crippling the government’s ability to distribute important information quickly. Two-way communications services are essential to the operation of the nation’s public safety answering points and 911 emergency call system for transmission of both voice and data.²¹⁶ These risks exist regardless of a provider’s size, as small service providers may serve critical infrastructure operators, and wireless service providers, broadcasters, and cable providers of all sizes are responsible for providing emergency alerts.

Second, Communications Sector assets historically have been targeted by malicious cyber actors. Per the 2023 IBM Security X Force Threat Intelligence Index, “Media and Telecom” entities have consistently experienced cyber incidents over the years, with the industry peaking as the industry experiencing the fourth most incidents in 2019.²¹⁷ Additionally, per the 2024 Homeland Security Threat Assessment, the telecommunications industry is likely to remain a target of foreign government-affiliated cyber actors from foreign countries such as Russia and China.²¹⁸

Finally, communications services also are essential to the operations of every other critical infrastructure sector. As noted in the Communications SSP, “the Communications Sector is one of the few sectors that can affect all other sectors. At a minimum, each sector depends on services from the

Communications Sector to support its operations. . . .”²¹⁹ Damage, disruption, or unauthorized access to these communications providers has a high likelihood of disrupting the reliable operation of other critical infrastructure assets, which can cause potentially cascading impacts to NCFs. This criticality to other sectors is reinforced by the fact that communications is one of four designated lifeline functions, indicating that the reliable operations of this sector is so critical that a disruption or loss of this function will directly affect the security and resilience of critical infrastructure within and across numerous sectors.²²⁰

c. Critical Manufacturing Sector

CISA is proposing to include in the description of a covered entity any entity that owns or has business operations that engage in one or more of the listed categories of manufacturing, which are the four manufacturing industries that together currently constitute the Critical Manufacturing Sector. The Critical Manufacturing Sector subsectors, which were identified by DHS after a study of the manufacturing sector, are Primary Metal Manufacturing (NAICS Subsector 331); Machinery Manufacturing (NAICS Subsector 333); Electrical Equipment, Appliance, and Component Manufacturing (NAICS Subsector 335); and Transportation Equipment Manufacturing (NAICS Subsector 336).²²¹ In 2008, DHS combined these four subsectors into a new Critical Manufacturing Sector based largely on the fact that the failure or disruption of any of these industries could cause, among other things, a large number of fatalities, significant national economic impact, or an inability of the government to provide necessary services to the public.²²²

Consideration of the factors enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of the entities comprising the Critical Manufacturing Sector within the description of covered entity. First, as noted in the previous paragraph, the President designated entities within these NAICS codes as the Critical Manufacturing Sector due in

²¹⁵ E.O. 13618—Assignment of National Security and Emergency Preparedness Communications Functions, 77 FR 40779 (July 6, 2012).

²¹⁶ Public safety answering points are required to report outages to the FCC pursuant to 47 CFR part 4, which the FCC then shares with CISA.

²¹⁷ IBM, 2023 IBM Security X-Force Threat Intelligence Index at 42, available at <https://www.ibm.com/reports/threat-intelligence> (hereinafter, “IBM 2023 Threat Index”).

²¹⁸ 2024 Homeland Security Threat Assessment at 20, *supra* note 188, at 20 (“Russian government-affiliated cyber espionage likely will remain a persistent threat to federal, state, and local governments, as well as entities in the defense, energy, nuclear, aviation, transportation, healthcare, education, media, and telecommunications industries. Chinese government cyber actors likely will continue to target key critical infrastructure sectors in the United States, including healthcare and public health, financial services, the defense industrial base, government facilities, and communications.”).

²¹⁹ Communications SSP, *supra* note 214, at 9.

²²⁰ See *Guide to Critical Infrastructure Security and Resilience*, *supra* note 198, at 4 (“There are four designated lifeline functions—transportation, water, energy, and communications, which means that their reliable operations are so critical that a disruption or loss of one of these functions will directly affect the security and resilience of critical infrastructure within and across numerous sectors.”).

²²¹ See 73 FR 23476 (Apr. 30, 2008).

²²² *Id.*

²¹⁴ See *Communications SSP: An Annex to the NIPP 2013* at 3 (2015), available at <https://www.cisa.gov/2015-sector-specific-plans> (hereinafter “Communications SSP”).

large part to the potential that disruption or compromise of such entities could impact national security, economic security, or public health and safety.²²³ Moreover, the entities within this sector often focus on efficiency, not redundancy, with lean inventories and just-in-time practices that can increase vulnerability to cascading disruptions and decrease agility in response with potentially damaging financial implications,²²⁴ increasing the likelihood that a cyber incident could negatively impact economic security.

Second, the manufacturing industry historically have been targeted by malicious cyber actors, and the expectation is for that targeting to continue. According to the IBM Security X-Force Threat Intelligence Index for 2023 (IBM 2023 Threat Index), the manufacturing industry experienced the most cyber incidents in both 2021 and 2022.²²⁵

Third, damage or disruption to a Critical Manufacturing Sector entity has the potential to disrupt the reliable operation of critical infrastructure. As noted in the *Designation of the National Infrastructure Protection Plan Critical Manufacturing Sector*, “[b]ecause of the importance of the manufacturing industry in sustaining cross-sector interdependencies, the Critical Manufacturing Sector also includes systems and operations that, if attacked or disrupted, would cause major interruptions to the essential functions of one or more other [critical infrastructure] sectors and result in national-level impacts.”²²⁶ Moreover, local or regional disruptions to entities within the Critical Manufacturing Sector can have cascading impacts across wide geographic regions and industries.²²⁷

Given the overall criticality of the entities within this sector, the reliance on NCFs on the items manufactured by entities within this sector, the relative lack of substitutability of many of the products produced by the sector, and the history of cyber incidents impacting manufacturing entities, CISA believes it is appropriate for all entities operating in any of the four Critical Manufacturing Sector subsectors to be required to report covered cyber incidents and ransom payments to CISA.

d. Defense Industrial Base Sector

CISA proposes including within the description of covered entity any entity that is a contractor or subcontractor required to report cyber incidents to DOD pursuant to the definitions and requirements of the DFARS *Safeguarding Covered Defense Information and Cyber Incident Reporting* clause located at 48 CFR 252.204–7012. This proposed sector-based criteria would require reporting from DOD contractors and subcontractors that provide operationally critical support to DOD, as well as DOD contractors and subcontractors that utilize unclassified information systems that are owned, or operated by or for, the contractor to process, store, or transmit covered defense information.²²⁸

DOD’s contractor cyber incident reporting requirements apply to the subset of contractors that process, store, or transmit “covered defense information” or that DOD has determined provide “operationally critical support.” “Covered defense information” includes things such as controlled technical information, critical information related to operations security, and information concerning certain items, commodities, technology, or software whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives.²²⁹ Contractors that provide “operationally critical support” include those that provide “supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.”²³⁰ CISA acknowledges that contractors that provide operationally critical support also includes entities in one or more critical infrastructure sectors, and are not generally considered as part of the Defense Industrial Base, as described in the Defense Industrial Base SSP.²³¹ For the

purposes of the CIRCIA rule, CISA proposes grouping these entities under the Defense Industrial Base Sector sector-based criteria to provide these entities an easier means of identifying whether they are a covered entity. CISA also recognizes that certain contractors that provide operationally critical support may fall under other proposed Applicability criteria, including other sector-based criteria (e.g. for the Transportation Sector).

As both DOD and their prime contractors frequently contract with small businesses to meet small business contracting and subcontracting goals and requirements, many of the entities covered under these criteria would not be captured by the size threshold contained in the proposed Applicability section. In developing the final rule requiring these contractors to report cyber incidents to DOD, DOD specifically addressed the need to include small businesses in the regulated population, stating in part that the costs to the nation in lost intellectual property and lost technological advantage over potential adversaries is much greater than the costs of implementation of the regulation and that “[t]he value of the information (and impact of its loss) does not diminish when it moves to contractors (prime or sub, large or small).”²³²

Consideration of the factors enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of these entities within the description of covered entity. First, cyber incidents perpetrated against contractors covered under the DFARS regulation “may cause harm to the Government through the compromise of covered defense information or other Government data, or the loss of operationally critical support capabilities, which could directly impact national security.”²³³ Second, members of the U.S. intelligence community have concluded that malicious cyber actors, to include foreign countries, are likely to continue to target members of the Defense Industrial Base Sector.²³⁴ Finally, damage, disruption, or unauthorized access to these entities, including the accessing of sensitive cybersecurity

critical-infrastructure-sectors/defense-industrial-base-sector.

²³² 81 FR 72986, 72987 (Oct. 21, 2016).

²³³ See 80 FR 51739 (Aug. 26, 2015).

²³⁴ See *2024 Homeland Security Threat Assessment* at 20, *supra* note 188, at 20 (“Russian government-affiliated cyber espionage likely will remain a persistent threat to . . . entities in the defense . . . industr[y]. Chinese government cyber actors likely will continue to target key critical infrastructure sectors in the United States, including . . . the defense industrial base. . . .”).

²²⁸ See 48 CFR 252.204–7012.

²²⁹ 48 CFR 204.7301.

²³⁰ 48 CFR 252.204–7012(a).

²³¹ The Defense Industrial Base Sector “consists of government and private sector organizations that can support military operations directly; perform R&D; design, manufacture, and integrate systems; and maintain depots and service military weapons systems, subsystems, components, subcomponents, or parts—all of which are intended to satisfy U.S. military national defense requirements.” *Defense Industrial Base Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan* at 15 (2015), available <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/>

²²³ *Id.*

²²⁴ See *Critical Manufacturing SSP: An Annex to the NIPP 2013* at 4 (2015), available at <https://www.cisa.gov/2015-sector-specific-plans> (hereinafter “*Critical Manufacturing SSP*”).

²²⁵ See *IBM 2023 Threat Index*, *supra* note 217, at 42; see also *Verizon 2022 DBIR*, *supra* note 181, at 50 (listing Manufacturing as experiencing the fifth most cyber incidents of any industry in 2022).

²²⁶ 73 FR 23476, 23477 (Apr. 30, 2008).

²²⁷ See *Critical Manufacturing SSP*, *supra* note 224, at v.

vulnerability information, may enable the disruption of the reliable operation of critical infrastructure because of its interdependency with critical defense infrastructure. As noted earlier, the entities proposed for inclusion under this sector-based criterion are regulated under the DFARS because they provide “operationally critical support” or process, store, or transmit “covered defense information.” Disruption of operationally critical support definitionally disrupts the reliable operation of critical defense infrastructure, and the compromise of covered defense information could be used to enable the disruption of the reliable operation of critical infrastructure.

CISA recognizes that entities required to report under these criteria are, by definition, already required to report certain cyber incidents to DOD. Given their criticality to national security, however, CISA nevertheless is proposing to include them within the CIRCIA Applicability section. This will ensure that the Federal government receives information necessary to identify cyber threats, exploited vulnerabilities, and TTPs that affect entities in this community and in other interdependent critical infrastructure sectors, even if changes are made to what must be reported pursuant to the DFARS regulation, over which CISA has no authority. CISA acknowledges the potential this creates for duplicative reporting and is committed to working with DOD to explore the applicability of the substantially similar reporting exception to enable entities subject to both CIRCIA and DFARS cyber incident reporting requirements to be able to comply with both regulatory reporting regimes through the submission of a single report to the Federal government to the extent practicable. Additional information on the substantially similar reporting exception can be found in Section IV.D.i in this document.

e. Emergency Services Sector

CISA proposes including within the description of covered entity any entity that provides one or more of five listed emergency services or functions to a population equal to or greater than 50,000 individuals. These five disciplines—law enforcement, fire and rescue services, emergency medical services, emergency management, and public works that contribute to public health and safety—and the types of entities that provide these services are

described in the 2015 Emergency Services SSP.²³⁵

Consideration of the factors enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of these entities within the description of covered entity. Regarding the first and third enumerated factors (consequence and disruption of reliable operation of critical infrastructure), as noted in the Emergency Services SSP, this sector’s operations provide the first line of support for nearly all critical infrastructure, and a failure or disruption in these services could result in significant harm or loss of life, major public health impacts, long term economic loss, and cascading disruptions to other critical infrastructure.²³⁶ Similarly, members of the broader public rely on these entities to provide assistance in the times of greatest need.

Regarding the second factor enumerated in 6 U.S.C. 681b(c)(1), which relates to threat, Emergency Services Sector entities routinely are targeted by malicious cyber actors. As noted in the 2012 Emergency Services Sector Cyber Risk Assessment Fact Sheet, Emergency Services Sector entities “face[] threats from criminals, hackers, terrorists, and nation-states, all of whom have demonstrated varying degrees of capability and intention to attack [Emergency Services Sector] cyber infrastructure.”²³⁷ Malicious cyber activity targeting law enforcement and other Emergency Services Sector entities has continued to be a problem in more recent years.²³⁸ Given Emergency Services Sector entities’ critical role in the nation’s public health and security and their continued targeting by malicious cyber actors, it is essential that CISA, as the SRMA for this sector, have an adequate

²³⁵ DHS, *Emergency Services SSP: An Annex to the NIPP 2013* (2015), available at <https://www.cisa.gov/resources-tools/resources/emergency-services-sector-specific-plan-2015>.

²³⁶ See *id.* at 3–7.

²³⁷ DHS, *2012 Emergency Services Sector Cyber Risk Assessment Fact Sheet*, available at <https://www.cisa.gov/resources-tools/resources/emergency-services-sector-cyber-risk-assessment>.

²³⁸ See, e.g., Resecurity, *Cybercriminals Are Targeting Law Enforcement Agencies Worldwide* (Aug. 19, 2022) (“Resecurity registered an increase in malicious activity targeting law enforcement agencies at the beginning of Q2 2022.”), available at <https://www.resecurity.com/blog/article/cybercriminals-are-targeting-law-enforcement-agencies-worldwide/>; J.J. Green, *Cyberterrorists Targeting First Responders* (Sept. 6, 2017) (“A U.S. intelligence community collaborative warned first responders in late July about escalating efforts to target them and their missions by cyberterrorists.”), available at <https://wtop.com/national-security/2017/09/cyber-terrorists-targeting-first-responders/>.

understanding of emerging cyber threats and trends impacting this sector.

Generally speaking, entities within the Emergency Services Sector are not subject to any Federal cyber incident reporting requirements. While most of the entities within this sector are SLTT entities likely to be captured by the SLTT Government Facilities Sector sector-based criterion (see Section IV.B.iv.2.h in this document), without this sector-based criterion, CISA would not receive reports from those Emergency Services Sector entities within the private sector that fall under the SBA Size Standards referenced in the sized-based standard in the Applicability section. Accordingly, to ensure CISA has both visibility into cyber incidents impacting privately owned Emergency Services Sector entities as well sufficient reporting from this sector overall, CISA is proposing this sector-based criteria.

Much like any other sector, entities within the Emergency Services Sector can vary greatly in size and resources. For the same reasons provided above as support for the proposal to use a size-based threshold, CISA believes that it makes sense to focus CIRCIA covered cyber incident and ransom payment reporting requirements on the larger, better-resourced entities within the Emergency Services Sector. To achieve that, CISA is proposing that the reporting requirements only apply to those entities that support populations equal to or greater than 50,000 individuals. CISA based its decision to propose 50,000 individuals as the threshold as that is consistent with the definition of a “small government jurisdiction” under the Regulatory Flexibility Act, which is the primary law requiring Federal departments and agencies to consider the effects of their regulations on small businesses and other small entities. 5 U.S.C. 601(5). CISA believes this is an appropriate basis for reporting under CIRCIA for the same reasons described in Section IV.B.iv.1.a as support for the size-based criterion.

f. Energy Sector

CISA proposes including within the description of covered entity any entity that is required to report cybersecurity incidents under NERC’s CIP Reliability Standards or required to file an Electric Emergency Incident and Disturbance Report OE-417 form, or any successor form, to DOE. This criterion proposes to require reporting from entities registered with NERC who are part of the BES and identified as “Responsible Entities” under CIP-003-8 (Cyber Security—Security Management Controls) or CIP-

008–6 (Cyber Security—Incident Reporting and Response Planning) and any successor standards. The goal of the CIP Cyber Security Standards is to mitigate the risk to the reliable operation of the BES as the result of a cybersecurity incident. This criterion would also require reporting from Electric Utilities, Balancing Authorities, Reliability Coordinators, and Generating Entities that are subject to electric emergency incident and disturbance reporting requirements via Form OE–417. DOE uses Form OE–417 to collect information from the electric power industry relevant to DOE’s overall national security and National Response Framework responsibilities. CISA is proposing to include this specific criterion in light of the importance of these Energy Sector assets and the frequency with which the energy industry is impacted by cyber incidents.

Consideration of the factors enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of these entities within the description of covered entity. Regarding the first and third enumerated factors (consequence and disruption of reliable operation of critical infrastructure), the reliable operation of the U.S. electric energy supply systems and BES is essential, as infrastructure within all 16 critical infrastructure sectors relies on electricity to function. As noted in the 2015 Energy SSP, “[t]he energy infrastructure provides essential fuel to all critical infrastructure sectors, and without energy, none of them can operate properly. Thus the Energy Sector serves one of the four lifeline functions, which means that its reliable operation is so critical that a disruption or loss of energy function will directly affect the security and resilience of other critical infrastructure sectors.”²³⁹ Cyber incidents affecting entities that own or operate the Energy Sector assets identified in the proposed criterion could result in cascading impacts affecting the nation’s ability to carry out a multitude of NCFs, with significant consequences to economic security and public health and safety.

Regarding the second factor enumerated in 6 U.S.C. 681b(c)(1) relating to threat, Energy Sector entities routinely are targeted by malicious cyber actors, including foreign actors. According to the IBM 2023 Threat Index, the energy industry experienced the fourth most cyber incidents between 2018 and 2022.²⁴⁰ The energy industry also is one of the industries noted in the

2024 Homeland Security Threat Assessment as likely to remain a target of Russian government-affiliated cyber espionage.²⁴¹

The criterion proposed captures a wide variety of Energy Sector entities, to include both energy generators and distributors across the spectrum of coal, natural gas, hydroelectric, wind, and solar. Many additional Energy Sector entities would be required to report under the proposed size-based threshold or other proposed sector-based criteria, such as the criteria requiring reporting from owners and operators of commercial nuclear power reactors and certain pipelines (see Sections IV.B.iv.2.k and l in this document).

CISA acknowledges the potential for the inclusion of this criterion to create an additional reporting obligation on entities already required to report cyber incidents to the Federal government. CISA is committed to working with DOE, FERC, and NERC to explore the applicability of the substantially similar reporting exception to enable, to the extent practicable, entities subject to both CIRCIA and CIP Reliability Standards or Form OE–417 reporting requirements to be able to comply with both regulatory reporting regimes through the submission of a single report to the Federal government. Additional information on the substantially similar reporting exception can be found in Section IV.D.i in this document.

When developing the sector-based criteria for the Energy Sector, CISA also considered developing a criterion focused on entities within the Energy Sector’s Oil and Natural Gas Subsector. The Oil and Natural Gas Subsector includes entities engaged in the production, gathering, processing, transmission, distribution, and storage of oil and gas, such as wells, processing plants and refineries, gathering and boosting stations, and natural or manmade storage facilities.²⁴² CISA anticipates that many Oil and Natural Gas Subsector entities will be considered covered entities through the size-based threshold, and that many others will be captured under any of a number of other proposed sector-based criteria, such as the Chemical Sector sector-based criterion covering entities that own or operate CFATS facilities, the Transportation Systems Sector sector-based criterion covering entities that own or operate MTSA facilities,

and the Transportation Systems Sector sector-based criterion covering entities that own or operate certain designated pipelines (see Sections IV.B.iv.2.a and l in this document). In light of the number of Oil and Natural Gas Subsector entities that CISA anticipates will be covered through these other criteria, CISA is not proposing a specific sector-based criterion for this subsector. However, if as a result of public comment, CISA determines that it must modify or eliminate any aspect of the description of covered entity through which Oil and Natural Gas Subsector entities currently would be included as part of this proposed rule, including the size-based criterion, CISA may incorporate a sector specific criterion or multiple criteria focused on Oil and Natural Gas Subsector entities in the final rule to ensure these entities remain covered entities.

If CISA were to include a specific Oil and Natural Gas Subsector sector-based criterion, it would likely set a threshold for Oil and Natural Gas Subsector entities and only those entities that exceed a specific size threshold would be considered a covered entity. Such a threshold would be set by CISA to ensure that the largest Subsector entities would be required to report, similar to the scope of entities that would be required to report under the proposed SBA size-based criterion, and could likely leverage the SBA Table of Size Standards employee or annual revenue thresholds using NAICS codes applicable to the Subsector to create an average that would become the threshold. CISA may also consider creating a threshold based on metrics specific to entities that are part of the Oil and Natural Gas Subsector, such as those entities exceeding specified refinery production capacity or liquefied natural gas terminal storage capacity.

CISA is interested in receiving comments from the public on the following topics:

12. CISA’s proposal to incorporate Oil and Natural Gas Subsector entities primarily through the size-based threshold instead of developing one or more criteria specifically targeting Oil and Natural Gas Subsector entities—and whether this size threshold will capture the correct population of entities in this subsector.

13. The potential alternative criteria that could be included if any of the current proposed criteria that would otherwise capture Oil and Natural Gas Subsector entities were modified or not included in the final rule.

²³⁹ Energy SSP at 19 (2015), available at <https://www.cisa.gov/2015-sector-specific-plans>.

²⁴⁰ IBM 2023 Threat Index, *supra* note 217, at 42.

²⁴¹ 2024 Homeland Security Threat Assessment, *supra* note 188, at 20.

²⁴² See EPA, Overview of the Oil and Natural Gas Industry, <https://www.epa.gov/natural-gas-star-program/overview-oil-and-natural-gas-industry> (last visited on Nov. 28, 2023).

g. Financial Services Sector

CISA proposes to include in the description of covered entity various Financial Services Sector entities that, if victimized in a covered cyber incident, have the potential to impact the economic security of the nation. Specifically, CISA is proposing to include in the description of covered entity (1) all of the Financial Services Sector entities that are required to report cybersecurity incidents to their respective primary Federal regulator (e.g., national banks; savings and loans holding companies; FICUs), (2) Financial Services Sector entities for whom the primary Federal regulator has indicated an intention to require cybersecurity incident reporting (e.g., futures commission merchants; ²⁴³ security-based swap data repositories), and (3) Financial Services Sector entities encouraged or expected to report cybersecurity incidents to their primary Federal regulator pursuant to an Advisory Bulletin (e.g., Fannie Mae and Freddie Mac; ²⁴⁴ money services businesses).²⁴⁵

CISA believes the inclusion of these entities in the description of covered entity is supported by consideration of the factors enumerated in 6 U.S.C. 681b(c)(1). As noted by many of the regulatory agencies currently requiring cyber incident reporting from Financial Services Sector entities, requiring the proposed entities to report helps promote early awareness of emerging threats to the financial system, and allows entities and their primary regulators to react to any such threats before they become systemic and threaten the nation's economic security.²⁴⁶ This is especially important

²⁴³ See Testimony of CFTC Chairman Rostin Behnam on the "State of the CFTC," U.S. House of Representatives Committee on Agriculture (Mar. 31, 2022), available at https://agriculture.house.gov/uploadedfiles/behnam_testimony_house_ag_3-31-2022.pdf.

²⁴⁴ Pursuant to *Advisory Bulletin 2020-05*, Fannie Mae and Freddie Mac are expected to report certain cybersecurity incidents to the FHFA. See *AB 2020-05: Enterprise Cybersecurity Incident Reporting* (Aug. 21, 2020), available at <https://www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Enterprise-Cybersecurity-Incident-Reporting.aspx>.

²⁴⁵ Pursuant to *Advisory Bulletin FIN-2016-A005*, money services businesses are expected to report certain cybersecurity incidents to the Department of the Treasury's Financial Crimes Enforcement Network. See *FIN-2016-A005, Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime* (Oct. 25, 2016), available at <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005>.

²⁴⁶ See, e.g., 86 FR 66424, 66424 (Nov. 23, 2021) ("This requirement will help promote early awareness of emerging threats to banking organizations and the broader financial system. This early awareness will help the agencies react to these threats before they become systemic."); 88 FR

given the continued targeting of Financial Services Sector entities by malicious cyber actors, as relevant to the second factor enumerated in 6 U.S.C. 681b(c)(1) related to threat. According to the IBM 2023 Threat Index, Financial Services Sector entities have experienced either the most or second most cyber incidents for each of the past five years,²⁴⁷ while the 2024 Homeland Security Threat Assessment highlights financial services as one of the sectors Chinese government cyber actors are likely to continue targeting.²⁴⁸ As to the third factor, i.e., the extent to which damage, disruption, or unauthorized access will likely enable the disruption of the reliable operation of critical infrastructure, systemic impacts to the Financial Services Sector has the potential to disrupt the reliable operation of critical infrastructure in light of virtually every critical infrastructure sectors' reliance on financial services entities for the conduct of day-to-day business operations.

As with several other proposed sector-based criteria, CISA recognizes that entities that would be required to report under these criteria are, for the most part, already required to report to another Federal regulatory agency. Given their importance to the nation's economy and the frequency with which they are targeted, CISA nevertheless is proposing to include them within the CIRCIA Applicability section ensure that the Federal government is able to receive information necessary to identify cyber threats against, exploited vulnerabilities of, and TTPs used to effect entities in this community without reliance on other authorities whose primary focus may not be security, and who might not currently or in the future require the submission of information necessary for CISA to achieve the purposes for which CIRCIA was enacted. CISA acknowledges the potential this creates for duplicative

12811, 12811 (Mar. 1, 2023) ("[G]iven the growing frequency and severity of cyber incidents within the financial services industry, it is important that the NCUA receive timely notice of cyber incidents that disrupt a FICU's operations, lead to unauthorized access to sensitive data, or disrupt members' access to accounts or services."); 88 FR 23146, 23147 (Apr. 14, 2023) ("[T]he regulation requires that SCI entities have policies and procedures reasonably designed to ensure that their systems have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain their operational capability and promote the maintenance of fair and orderly markets. . . .").

²⁴⁷ *IBM 2023 Threat Index*, supra note 217, at 42; see also Verizon 2022 DBIR, supra note 181, at 50 (noting the Finance industry had the third highest number of incidents in 2022).

²⁴⁸ *2024 Homeland Security Threat Assessment*, supra note 188, at 20.

reporting and is committed to working with the respective Financial Services Sector Federal regulatory agencies to explore the applicability of the substantially similar reporting exception to enable, to the extent practicable, entities subject to both CIRCIA and another reporting requirement to be able to comply with both regulatory reporting regimes through the submission of a single report to the Federal government. Additional information on the substantially similar reporting exception can be found in Section IV.D.i in this document.

h. Government Facilities Sector

CISA proposes to include three different sector-based criteria for entities in the Government Facilities Sector, one focused on SLTT Government Entities, one focused on Education Subsector entities, and one focused on Elections Infrastructure Subsector entities. First, CISA proposes to include in the description of covered entity any SLTT Government entity for a jurisdiction with a population equal to or greater than 50,000 individuals. Second, CISA proposes to include in the description of covered entity any entity that qualifies as either (A) a local educational agency (LEA), educational service agency (ESA), or state educational agency (SEA), as defined under 20 U.S.C. 7801, with a student population of 1,000 or more students; or (B) an institute of higher education (IHE) that receives funding under Title IV of the Higher Education Act. Third, CISA is proposing to include in the description of covered entity any entity that manufactures, sells, or provides managed service for information and communications technology specifically used to support election processes or report and display results on behalf of SLTT governments, including but not limited to voter registration databases; voting systems; and information and communication technologies (ICT) used to report, display, validate, or finalize election results. As discussed in greater detail in Section IV.D.iii in this document, CISA is proposing to except from required reporting Federal agencies already required to report incidents to CISA under FISMA, such that these sector-based criteria are focused on SLTT and private sector members of the Government Facilities sector.

With the first of these three criteria, CISA is seeking reporting from SLTT Government Entities from jurisdictions over a certain size. Consideration of the factors enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of larger SLTT Government Entities in the description of covered entity. Regarding

the first factor, it is likely that the disruption or compromise of only some of the largest SLTT Government Entities have the potential to cause significant consequences on a large enough scale to impact national security, economic security, and, especially, public health and safety. SLTT Government Entities are responsible for numerous NCFs within their jurisdictions, overseeing functions such as developing and maintaining public works and services, preparing for and managing emergencies, and preserving constitutional rights. Similarly, along with their Federal counterparts, SLTT Government Entities like State Departments of Health provide a wide variety of services that are critical to the public health and well-being of their citizenry.

As to the second factor CISA is to consider, *i.e.*, the likelihood that such an entity will be targeted by a malicious cyber actor, SLTT Government Entities are frequently impacted by cyber incidents.²⁴⁹ Furthermore, the 2024 Homeland Security Threat Assessment indicates that SLTT Government Entities are likely to remain the targets of foreign governments, such as Russia and China.²⁵⁰

Third, damage or disruption to various SLTT Government Entities have the potential to disrupt the reliable operation of critical infrastructure. SLTT Government Entities own or operate critical infrastructure across various sectors, to include energy, water, transportation, and emergency services among others. Damage or disruption of these entities has potential to directly impact the reliable operation of critical infrastructure and to create the potential for cascading impacts affecting the reliable operations of other critical infrastructure as well.

For the same reasons that CISA is proposing to limit the Emergency Services Sector sector-based criteria to entities that serve populations equal to or greater than 50,000 individuals (see Section IV.B.iv.2.e), CISA is proposing to use the same small government jurisdiction threshold to demarc which SLTT jurisdictions' government entities

²⁴⁹ See, *e.g.*, *Verizon 2022 DBIR*, *supra* note 181, at 50 (public administration entities experienced the second largest number of reported incidents); *IBM 2023 Threat Index*, *supra* note 217, at 42 (listing Government as the eighth most impacted industry).

²⁵⁰ See *2024 Homeland Security Threat Assessment*, *supra* note 188, at 20 (“Russian government-affiliated cyber espionage likely will remain a persistent threat to federal, state, and local governments [and] Chinese government cyber actors likely will continue to target key critical infrastructure sectors in the United States, including . . . government facilities.”).

will be required to report. CISA believes that this line of demarcation, which would provide regulatory relief to more than two-thirds of counties and over 95% of cities from which CISA could require reporting under the statutory definition of covered entity, should cover enough entities to provide sufficient data for CISA to perform cyber incident trend and threat analysis for this vital community.

With the second of these criteria—covering LEAs, ESAs, and SEAs with student populations of 1,000 or more students, as well as IHE that receive funding under Title IV of the Higher Education Act—CISA seeks to ensure reporting from a sufficient cross-sector of entities to understand and be able to share information on threats to our nation’s education facilities. Consideration of the factors enumerated in 6 U.S.C 681b(c)(1) supports the inclusion of these entities within the description of covered entity, especially the second factor related to threat.

As noted in the 2024 Homeland Security Threat Assessment, “[Kindergarten through 12th grade (K–12)] school districts have been a near constant ransomware target due to school systems’ IT budget constraints and lack of dedicated resources, as well as ransomware actors’ success at extracting payment from some schools that are required to function within certain dates and hours.”²⁵¹ The Verizon 2022 DBIR and the IBM 2023 Threat Index both identified education facilities as the sixth most frequently impacted industry in 2022.²⁵² A recent U.S. GAO report on cybersecurity at K–12 schools echoed this conclusion, stating that “research from several federal and private sector sources indicate that cyber threats [against K–12 schools] have escalated over time, and are becoming more sophisticated and pervasive.”²⁵³ Many Education Subsector entities, primarily IHE, also own infrastructure or perform activities that support national security, public health and safety, and the reliable operations of critical infrastructure, such as hospitals, first responder organizations, water and wastewater treatment facilities, energy facilities, and research facilities.

To obtain reporting from a representative cross-section of

²⁵¹ See *2024 Homeland Security Threat Assessment*, *supra* note 188, at 18.

²⁵² *Verizon 2022 DBIR*, *supra* note 181, at 50; *IBM 2023 Threat Index*, *supra* note 217, at 42.

²⁵³ U.S. GAO, *GAO–23–105480, Critical Infrastructure Protection: Additional Federal Coordination is Needed to Enhance K–12 Cybersecurity* at 12 (2022), available at <https://www.gao.gov/products/gao-23-105480>.

Education Subsector entities, CISA proposes two prongs to the criterion for this subsector, one focused on the K–12 community and one focused on IHE. For the K–12 community, CISA proposes to require reporting from LEAs, ESAs, and SEAs, as defined in 20 U.S.C. 7801 (part of the Elementary and Secondary Education Act, as amended (20 U.S.C. 6301 *et seq.*)), with a student population of 1,000 or more students. LEAs, more commonly referred to as school districts, are the public authorities legally constituted within a State for administrative control or direction of public schools in a city, county, township, school district, or other political subdivision of a State.²⁵⁴ SEAs are the Statewide board of education or other agency or officer primarily responsible for the supervision of schools within a state.²⁵⁵ ESAs are state-authorized regional service centers that often provide direct education service delivery to schools and districts in their respective regions.

CISA proposes to require reporting from LEAs, SEAs, and ESAs with student populations of 1,000 or more students. This threshold would capture in the description of covered entities all SEAs, approximately half of all LEAs, and some percentage of ESAs, with smaller LEAs and ESAs excluded from the reporting population.²⁵⁶

CISA is proposing this threshold, which is limited to LEAs, SEAs, and ESAs, with larger student populations, for three primary reasons. First, studies show that “larger school districts (as defined by student enrollment) appear to be at a significantly greater risk for experiencing a cyber incident than small school districts.”²⁵⁷ Second, covered cyber incidents impacting education agencies with larger student populations will, on average, have a greater likelihood of impacting more individuals, thus potentially causing more substantial impacts than incidents perpetrated against education agencies with smaller student populations. Finally, similar to the use of the small government jurisdiction definition as a

²⁵⁴ 34 CFR 303.23.

²⁵⁵ 34 CFR 300.41.

²⁵⁶ All SEAs (56 of 56) and approximately 52% of LEAs (6,911 of 13,318) have student populations of 1,000 or more students. See National Center for Education Statistics, 2022 Digest of Education Statistics, Table 214.20, available at https://nces.ed.gov/programs/digest/d22/tables/dt22_214.20.asp. As the student population covered by each ESA is not readily available, to be conservative, for purposes of the CIRCA RIA, CISA is assuming all 553 ESAs serve student populations of 1,000 or more students.

²⁵⁷ Douglas Levin, *The State of K–12 Cybersecurity: Year in Review—2022 Annual Report* at 15, available at <https://www.k12six.org/the-report>.

threshold line of demarcation for other SLTT Government Entities, CISA believes this approach will afford regulatory relief to smaller entities that are likely to have fewer resources with which to comply with CIRCIA's incident reporting requirements, while still requiring reporting from a broad enough population to provide sufficient data for CISA to perform cyber incident trend and threat analysis for this community.

In developing this criterion and threshold, CISA considered various alternatives, including (1) covering LEAs, SEAs, and ESAs with student populations of 2,500 students or more; (2) using the same small government jurisdiction threshold CISA is proposing to use for other SLTT Government Entities and entities required to report under the Emergency Services Sector sector-based criteria (*i.e.*, entities serving jurisdictions with a population of 50,000 or more individuals); and (3) requiring reporting from all LEAs, SEAs, and ESAs.

The first alternative CISA considered was establishing a higher threshold based on student population, specifically one that would require reporting from LEAs, SEAs, and ESAs with 2,500 or more students. Setting the threshold at 2,500 students would result in approximately 30% of all LEAs, SEAs, and ESAs collectively qualifying as covered entities.²⁵⁸ The primary benefit of this threshold, in comparison to the proposed 1,000 student threshold, would be the lower costs to the K–12 community resulting from having fewer entities qualify as covered entities. However, an analysis conducted by the Department of Education based on cyber incidents impacting the K–12 community that were voluntarily reported to CISA in 2023 showed that the greatest percentage of incidents impacting the K–12 community impacted school districts with between 1,000 and 2,500 students (around approximately 30% of all incidents). This represents the largest percentage of incidents experienced by any of the size-based segments of the K–12 community analyzed by the Department of Education.²⁵⁹ Given the large

percentage of cyber incidents impacting school districts with between 1,000 and 2,500 students, CISA believes the small additional burden imposed on the sector by requiring reporting from education agencies with between 1,000 and 2,500 students that experience a substantial cyber incident or make a ransom payment is outweighed by the benefit of the additional insight into cybersecurity threats targeting the K–12 community that this additional coverage would provide. Thus, CISA has elected to propose setting the student population threshold at 1,000 students, and not 2,500 students. CISA acknowledges that it may be possible to set this threshold at 2,500 students and get some reporting that would be informative to the overall subsector; however, CISA does not believe this will result in representative or adequate reporting for the subsector because it would not include the population that is most likely to be targeted by malicious actors based on the Department of Education's analysis. Nonetheless, CISA is interested in receiving comments on the proposal to set the threshold at 1,000 students versus 2,500 students for this subsector, and what benefits or disadvantages may exist for selecting one threshold over another.

Regarding the second alternative considered—*i.e.*, using the same jurisdiction-based threshold that CISA is proposing for other SLTT Government Entities—CISA sees value in using the same threshold across all SLTT Government Entities, which includes LEAs, SEAs, and ESAs. Doing so would avoid potential confusion resulting from having different thresholds for different types of SLTT Government Entities. However, based on consultations with the Department of Education, CISA understands that school districts frequently do not follow typical county, city, or other jurisdictional lines, with many LEAs and ESAs covering schools that are located in multiple jurisdictions. As a result, the number of individuals within a given LEA's or ESA's "jurisdiction" may not be readily available or discernable, causing many LEAs and ESAs to have difficulties in determining if they meet a criterion

based on the number of individuals located within their "jurisdiction." Conversely, student population is a standard metric used within the K–12 community for various purposes and is a metric with which every LEA, SEA, and ESA should be very familiar. As an entity's ability to determine whether it is a covered entity is crucial to implementation of the proposed regulation, CISA believes it is preferable to use a student population-based metric for the K–12 community rather than the jurisdictional population-based metric CISA is proposing for the sector-based criteria for other SLTT Government Entities.

Regarding the final alternative considered—*i.e.*, covering all LEAs, SEAs, and ESAs—there are some arguments in favor of broader reporting requirements, such as the frequency with which educational entities are subjected to cyber incidents and the absence of any other nationwide cyber incident reporting requirements for this community. Ultimately, however, CISA decided that, for the same reasons CISA is proposing a size threshold for the sector-based criteria for other SLTT Government Entities and several other sectors and subsectors, proposing a size threshold for the sector-based criteria for the K–12 community is the most well-supported approach. Doing so not only supports general consistency in approach across the SLTT Government Entities' community, but also promotes the correct balance between burden and ensuring sufficient reporting from this community.

CISA is interested in receiving comments on this prong of the proposed sector-based criteria, to include:

14. Whether CISA should include a size threshold for education agencies that would be required to report and, if so, what metric (*e.g.*, student population; number of individuals within the jurisdiction) should be used as the unit or measurement for the threshold.

15. If CISA were to include a criterion for education agencies using a size threshold based on student population, whether 1,000 students, 2,500 students, or another number of students would be the optimal threshold for this subsector criterion and why.

16. Whether CISA should include a criterion to require reporting from some or all private schools operating in the K–12 space, as cyber incidents impacting K–12 private schools would not be subject to reporting under the current proposal (unless they qualify as a covered entity under the general size-based threshold) since LEAs, SEAs, and

²⁵⁸ All SEAs (56 of 56) and approximately 28% of LEAs (3,726 of 13,318) have student populations of 2,500 or more students. See National Center for Education Statistics, 2022 Digest of Education Statistics, Table 214.20, available at https://nces.ed.gov/programs/digest/d22/tables/dt22_214.20.asp. As the student population covered by each ESA is not readily available, to be conservative, for purposes of the CIRCIA RIA, CISA is assuming all 553 ESAs serve student populations of 2,500 or more students.

²⁵⁹ Department of Education analyzed the incidents experienced by K–12 school districts with

the following size-based segments: 25,000 or more students; 10,000–24,999 students; 5,000–9,999 students; 2,500–4,999 students; 1,000–2,499 students; 600–999 students; 300–599 students; 1–299 students; and no size reported. Even combining some of the other segments, the 1,000–2,499 students segment still experienced a greater percentage of the analyzed incidents than other segments (*e.g.*, more than all of the smaller segments combined, more than the 2,500–4,999 and 5,000–9,999 students segments combined, and more than the 10,000–24,999 and 25,000 or more students segments combined).

ESAs do not have authority over private schools.

The Government Facilities Education Subsector sector-based criteria would also include in the description of covered entity those IHE that receive funding under Title IV of the Higher Education Act (Title IV). In addition to being part of a routinely targeted subsector, given the diverse roles IHE can play in various NCFs, the consequences of a covered cyber incident impacting an IHE could be significant. For example, some IHE provide research or other support to national security entities such as DOD and DHS, others are high-risk chemical facilities regulated under CFATS. While some IHE might be covered by the Applicability section based on other sector-based criteria, CISA believes it is important to require reporting from IHE more broadly.

IHE that receive funding under Title IV include any IHE—be it a college or university that offers a 2-year or 4-year degree, a trade school, or other type of IHE—that offers Federal financial aid to its students. This includes the majority of IHE, ensuring that CISA will receive adequate reporting to identify cybersecurity trends for the entire IHE community. Title IV-funded IHE also already are subject to cybersecurity incident reporting requirements under the Gramm-Leach-Bliley Act, but that is limited to reporting to the Department of Education cybersecurity incidents resulting in unauthorized access to student information. This proposal will expand the scope of reporting required of these IHE to reporting on a broader range of cybersecurity incidents and any ransom payments made by these entities.

With the third proposed Government Facilities Sector sector-based criteria—entities that manufacture, sell, or provide managed service for information and communications technology specifically used to support election processes or report and display results on behalf of SLTT governments, including but not limited to voter registration databases; voting systems; and ICT used to report, display, validate, or finalize election results—CISA is seeking to ensure sufficient reporting to understand cyberthreats to our nation's elections infrastructure and assist SLTT election officials and their private sector partners to prevent, respond to, and mitigate impacts of cyber incidents impacting elections infrastructure. In January 2017, DHS officially designated election infrastructure as a critical infrastructure subsector of the Government Facilities

Sector.²⁶⁰ In this designation, the Department stated that the United States' election infrastructure is vital to our national interest and must be a priority for cybersecurity assistance and protections provided by the Department.²⁶¹

Election infrastructure refers to storage facilities, polling places, and centralized vote tabulation locations used to support the election process, and ICT systems used to manage the election process and report and display results on behalf of SLTT governments. Such ICT systems include, but are not limited to, voter registration databases and other systems used to manage the voter registration process and maintain voter registration data; electronic poll books; voting systems, election management systems, and other systems used to create, print, facilitate the voting of, and tabulate ballots, including electronic ballot delivery, marking, and return systems, as well as systems used to validate, audit, certify, or otherwise finalize election results; and public information systems used to display election information and results to the public, including SLTT election websites and election night reporting systems. These and other types of technologies used to manage the election process are described in greater detail in the Election Infrastructure SSP.²⁶²

Currently, entities that manufacture, sell, or provide managed services for ICT specifically used to support election processes are not subject to any Federal cyber incident reporting requirements. Consequently, in conjunction with the first Government Facilities Sector sector-based criterion, which would require reporting from SLTT election entities for jurisdictions with populations greater than 50,000 individuals, CISA believes this third Government Facilities Sector sector-based criterion focused on private sector members of the Election Infrastructure Subsector is necessary to ensure CISA and its Federal partners receive sufficient reporting from both public and private sector entities within the Elections Infrastructure Subsector to

understand the cyber threats to elections infrastructure.

CISA believes that including these entities in the description of covered entity is supported by a consideration of the three factors enumerated in 6 U.S.C. 681b(c)(1) (*i.e.*, consequence, threat, and disruption of reliable operation of critical infrastructure). While damage or disruption of election infrastructure may not directly produce national security, economic security, or public health and safety consequences, the impact of eroded public confidence in our election system may indirectly lead to such consequences.²⁶³ Damage, destruction, or unauthorized access to elections infrastructure would impact the reliable operation of critical infrastructure as certain systems and assets of election infrastructure themselves are critical infrastructure.²⁶⁴ Finally, malicious cyber actors have targeted and are expected to continue to target elections infrastructure.²⁶⁵

CISA recognizes that many standard ICT, such as laptops, cell phones, email, staff management and payroll software, and business and data management software may be used by entities responsible for the conduct and management of elections. CISA does not intend for this sector-based criterion to capture entities that manufacture, sell, or provide managed services related to those types of ICT, except to the extent that they are specifically used for election processes. Thus, for example, while an entity that develops, sells, or provides managed services related to software specifically designed to facilitate the management of temporary election workers would be considered a covered entity under this proposed criterion, a standard staff management and payroll software provider would not be considered a covered entity simply

²⁶³ See *Final Report of the Select Committee to Investigate the January 6th Attack on the United States Capitol* (Dec. 22, 2022), available at <https://www.govinfo.gov/app/details/GPO-J6-REPORT/>.

²⁶⁴ Statement by Secretary Jeh Johnson, *supra* note 260 ("Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law.").

²⁶⁵ See *2024 Homeland Security Threat Assessment*, *supra* note 188, at 19 ("Our electoral processes remain an attractive target for many adversaries, and we expect many of them will seek to influence or interfere with the 2024 election . . . Cyber actors likely will seek to exploit election-related networks and data, including state, local, and political parties' networks and election officials' personal devices and email accounts. . . . Though we continue to strengthen the integrity of our elections infrastructure, cyber actors, both government-affiliated and cyber criminals, likely will remain opportunistic in their targeting of election-related networks and data, routinely attempting to exploit misconfigured or vulnerable public-facing websites, web servers, and election-related information technology systems.").

²⁶⁰ See Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017), available at <https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical> (hereinafter "Statement by Secretary Jeh Johnson").

²⁶¹ *Id.*

²⁶² *Election Infrastructure Subsector-Specific Plan: An Annex to the NIPP 2013* (2020), available at https://www.cisa.gov/sites/default/files/publications/election_infrastructure_subsector_specific_plan.pdf.

because an SLTT election office uses the software to conduct routine business.

i. Healthcare and Public Health Sector

CISA proposes to include in the description of covered entity²⁶⁶ multiple sector-based criteria related to the Healthcare and Public Health Sector. As its name implies, entities within the Healthcare and Public Health Sector, along with Federal and SLTT Departments of Health and similar government entities that are part of the Government Facilities Sector, are essential to the maintenance of the public health of the nation, providing goods and services that are integral to maintaining local, national, and global health security. Entities within the sector provide various services, to include direct patient care, medical equipment and materials, laboratory support, health IT, health plans, and mass fatality management services.²⁶⁷

Unfortunately, entities within this sector routinely experience cyber incidents, with U.S. healthcare entities experiencing the seventh most cyber incidents of any industry in 2022.²⁶⁸ Many entities within the sector currently are required to report certain cyber incidents to HHS under the HIPAA Breach Notification Rule (45 CFR 164.400–414) and to the Federal Trade Commission under the HITECH Act Health Breach Notification Rule (16 CFR 318); however, those requirements are generally focused solely on data breaches and do not require reporting of other types of cyber incidents that do not involve unauthorized acquisition of or access to personal health information. Device manufacturers, importers, distributors, and user facilities must establish and maintain records, make such reports, and provide such information, as the Secretary of Health and Human Services may by regulation reasonably require to assure that such device is not adulterated or misbranded and to otherwise assure its safety and effectiveness. 21 U.S.C. 360i(a). FDA's regulations at 21 CFR part 803 require device manufacturers and importers, to report certain device-related adverse

events and product problems, including those caused by cyber incidents, to the FDA, but that reporting requirement is limited to situations where a device is likely to or has caused or contributed to a death or serious injury or for medical device manufacturers and importers when they initiate a correction or removal of a medical device to reduce a risk to health posed by the device. In light of the sector's broad importance to public health, the diverse nature of the entities that compose the sector, the historical targeting of the sector, and the current lack of required reporting unrelated to data breaches or medical devices, CISA proposes requiring reporting from multiple parts of this sector.

The first criterion CISA proposes related to this sector will mean that certain entities providing direct patient care will be considered covered entities. Specifically, CISA proposes including in the description of covered entity any entity that owns or operates (1) a hospital, as defined by 42 U.S.C. 1395x(e), with 100 or more beds, or (2) a critical access hospital, as defined by 42 U.S.C. 1395x(mm)(1). Many different types of entities provide direct care to patients, such as hospitals, clinics, urgent care facilities, medical offices, surgical centers, rehabilitation centers, nursing homes, and hospices. The size of the facilities, the number of patients cared for daily, and the types of services provided can vary dramatically across these entities. While all of these various types of entities contribute to the nation's public health and well-being, CISA does not believe it is prudent or cost-effective to require covered cyber incident and ransom payment reporting from every individual provider of patient care. Rather, CISA is proposing to focus on hospitals, as they routinely provide the most critical care of these various types of entities, and patients and communities rely on them to remain operational, including in the face of cyber incidents affecting their devices, systems, and networks to keep them functioning.

Currently, there are approximately 6,000 hospitals in the United States.²⁶⁹ CISA is proposing requiring reporting from larger hospitals (*i.e.*, those with more than 100 beds) and critical access hospitals. CISA believes it is worthwhile to focus on larger hospitals for required reporting, as they are more likely than smaller hospitals to experience substantial impacts if they fall victim to a covered cyber incident

given their size and the correspondingly greater number of patients they are caring for on any given day. Additionally, focusing on larger hospitals is supported by much of the same rationale behind CISA's decision to propose an overall size-based criterion based on the SBA small business size standards in the Applicability section (*e.g.*, larger hospitals are more likely to have in-house or access to cyber expertise; larger hospitals are likely to be better equipped to simultaneously respond to and report a cyber incident).

While CISA is not generally proposing to require reporting from smaller hospitals, CISA is proposing to require reporting from critical access hospitals. Critical access hospitals are facilities that have been certified by the Centers for Medicare & Medicaid Services as meeting certain criteria, including that they are located in a state that has established a Medicare rural hospital flexibility program, and that they are designated as a critical access hospital by the State in which they are located, among other requirements.²⁷⁰ CISA is proposing to include these in the reporting requirements as they typically are the only source of emergency medical care for individuals living within certain rural areas. As a result, a substantial cyber incident at a critical access hospital may have disproportionate impacts to its size given the limited alternative emergency health care options for individuals within its service area.

The second public health and healthcare sector sector-based criterion CISA is proposing would require reporting from manufacturers of drugs listed in Appendix A of the report *Essential Medicines Supply Chain and Manufacturing Resilience Assessment*, sponsored by the U.S. Department of Health and Human Services (HHS) Administration for Strategic Preparedness and Response (ASPR).²⁷¹ In this report, ASPR, in collaboration with governmental and non-governmental entities, prioritized 86 essential medicines identified as either critical for minimum patient care in acute settings or important for acute care or important for acute care of respiratory illnesses/conditions, with no

²⁶⁶ CISA is aware that covered entity also is a defined term in the HIPAA regulations. As noted in the proposed § 226.1, the definitions included in this proposed rule are “[f]or the purposes of this Part.” Whenever the term covered entity is used in this document, it is referring to the statutory term in CIRCIA and/or the proposed definition of covered entity in the CIRCIA proposed rule, and not to entities that meet the existing HIPAA regulatory definition of covered entity or any other existing definition of the term covered entity.

²⁶⁷ See *Healthcare and Public Health SSP*, *supra* note 173.

²⁶⁸ See *IBM 2023 Threat Index*, *supra* note 217, at 42; *Verizon 2022 DBIR*, *supra* note 181, at 50.

²⁶⁹ See American Hospital Association, *Fast Facts on U.S. Hospitals*, <https://www.aha.org/statistics/fast-facts-us-hospitals> (last visited July 31, 2023).

²⁷⁰ See section 1820(e) of the Social Security Act and 42 CFR 485.601 *et seq.*

²⁷¹ ARMI, *Essential Medicines Supply Chain and Manufacturing Resilience Assessment* (May 2022), available at https://www.armi.usa.org/wp-content/uploads/2022/07/ARMI_Essential-Medicines-Supply-Chain-Report_508.pdf; see also ASPR, *Essential Medicines Report Now Available* (May 23, 2022), available at <https://aspr.hhs.gov/newsroom/Pages/Essential-Medicines-May22.aspx>.

comparable alternative available. The report was published in response to a commitment by the Biden Administration, in its June 2021 100-day review of the pharmaceutical supply chain as tasked in Executive Order 14017, to “assemble a consortium of public health experts (including emergency medicine and critical care) in the government, non-profit, and private sector to review [a previous list of Essential Medicines, Medical Countermeasures, Critical Inputs developed by FDA in response to Executive Order 13944], and recommend 50–100 drugs that are most critical to have available at all times for U.S. patients because of their clinical need and lack of therapeutic redundancy.”²⁷² Given the importance of these products, CISA believes it is appropriate to include manufacturers of these products among the CIRCIA covered entity population in order to enable the Federal government to more quickly identify any emerging cyberthreats against them.

Third, CISA is proposing to require reporting from manufacturers of Class II (moderate risk) and Class III (high risk) devices, as defined in 21 U.S.C. 360c. FDA has established classifications for approximately 1,700 different generic types of devices, each of which is assigned to one of three regulatory classes based on the level of control necessary to provide reasonable assurance of the safety and effectiveness of the device.²⁷³ These classifications are risk-based, with Class I devices presenting the lowest risk and Class III devices presenting the greatest risk.²⁷⁴ Based on discussions with FDA, CISA believes that requiring reporting from manufacturers of Class II and III devices provides a risk-based means balancing reporting from medical device manufacturers while supporting the collection of an adequate amount of reporting to understand cyber threats, vulnerabilities, and TTPs for this industry segment.

CISA believes that the inclusion of all three Healthcare and Public Health Sector sector-based criteria is supported by a consideration of the three factors enumerated in 6 U.S.C. 681b(c)(1) (*i.e.*, consequence, threat, and disruption of the reliable operation of critical

infrastructure). Regarding the first factor, consequence, disruption or compromise at any of these key sector assets has the potential for significant impacts to public health and safety. All hospitals play an important role in public health, but disruption or compromise impacting any of the hospitals CISA proposes to cover could have especially significant impacts on public health given the number of patients and types of services provided at large hospitals, and the fact that critical access hospitals may be the only source of emergency care in their immediate vicinity, sometimes for hundreds of miles. Similarly, a compromise or disruption resulting in unavailability, supply shortages, or compromise of essential medicines, medical countermeasures, or Class II and III medical devices has a significant potential for creating public health consequences on a scale that could impact all Americans. Regarding the second factor, threat, entities within the Healthcare and Public Health sector routinely experience cyber incidents.²⁷⁵ The DHS 2024 Homeland Security Threat Assessment indicates that threats against this sector include Russian and Chinese government-affiliated actors, who are likely to continue to target the healthcare and public health sector.²⁷⁶ Finally, regarding the third factor, the disruption of the reliable operation of critical infrastructure, the entities that would be covered under the criteria—large hospitals; critical access hospitals; manufacturers of essential medicines; and manufacturers of Class II and III medical devices—typically themselves are considered critical infrastructure. Moreover, as the COVID–19 pandemic demonstrated, significant events impacting the public health can have cascading effects that threaten the reliable operation of critical infrastructure across multiple sectors.

In establishing these proposed criteria, CISA also considered including criteria related to health insurance companies, health IT providers, and entities operating laboratories or other medical diagnostics facilities. Ultimately, CISA determined it was not necessary to include specific sector-based criteria for any of those three industry segments. In the case of health insurance companies and entities operating laboratories or other medical diagnostics facilities, CISA believes a sufficient number of entities already will be captured under the size-based

criterion that applies across all critical infrastructure sectors. However, if as a result of public comment, CISA determines that it must modify or eliminate any aspect of the description of covered entity through which health insurance companies and entities operating laboratories or other medical diagnostics facilities are currently captured as part of this proposed rule, including the size-based criterion, CISA may incorporate a sector-based criterion or multiple criteria focused on criteria capturing these entities as part of the final rule to ensure that they remain covered entities. If CISA were to include one or more sector-based criteria that would cover health insurance companies and laboratories and other medical diagnostics facilities, it would likely set a threshold based on annual revenue, number of employees, or some other metric and only entities that exceed the threshold would be considered covered entities. Such a threshold would be set by CISA to ensure that the largest of these types of entities would be considered covered entities and CISA likely would look at the SBA Size Standards for context and to develop relevant averages using NAICS codes applicable to such entities and may consult with the Healthcare and Public Health SRMA to develop the final criterion or criteria. Regarding the health IT community, CISA believes that the most common type of cyber incident such entities will face are data breaches. As data breaches are not the primary focus of CIRCIA, and those entities already are required to report data breaches of unsecured protected health information under the HIPAA Breach Notification Rule and personal health records under the HITECH Act Health Breach Notification Rule, CISA does not believe it is necessary to include a specific criterion focused on entities in the health IT industry.

CISA would be interested in receiving comments on:

17. The scope of entities that would and would not be considered covered entities based on the three criteria proposed by CISA, whether the scoping is appropriate, and what, if any, specific refinements should CISA consider related to any of the criteria.

18. The proposal to forgo including specific criteria focused on health insurance companies, health IT providers, and entities operating laboratories or other medical diagnostics facilities.

j. Information Technology Sector

CISA proposes including within the description of covered entity any entity that meets one or more of four proposed

²⁷² Dep’t of Health & Human Servs., *Review of Pharmaceuticals and Active Pharmaceutical Ingredients* at 243 (June 2021), available at <https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf>.

²⁷³ See FDA, *Classify Your Medical Device*, <https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device> (last visited July 24, 2023).

²⁷⁴ See *id.*

²⁷⁵ See *IBM 2023 Threat Index*, *supra* note 217, at 42; *Verizon 2022 DBIR*, *supra* note 181, at 50.

²⁷⁶ *2024 Homeland Security Threat Assessment*, *supra* note 188, at 20.

Information Technology (IT) Sector sector-based criteria. First, CISA proposes including within the description of covered entity any entity that knowingly provides IT hardware, software, systems, or services to the Federal government. Second, CISA proposes including within the description of covered entity any entity that has developed and continues to sell, license, or maintain any software that meets the definition of “critical software” as that term was defined by NIST pursuant to Executive Order 14028—Improving the Nation’s Cybersecurity (May 12, 2021). Third, CISA proposes to include within the description of covered entity, any entity that is an original equipment manufacturer (OEM), vendor, or integrator of OT hardware or software components. Fourth, CISA proposes to include within the description of covered entity any entity that performs functions related to domain name operations.

To conduct a cyber incident, malicious cyber actors seek to exploit some aspect of the IT Sector, through IT hardware, software, systems, or services. Moreover, given many IT providers’ positions in the critical infrastructure supply chain, their roles as cyber service providers (e.g., CSPs, managed service providers) to other entities, and their important role in the functioning of the internet, a covered cyber incident impacting a member of the IT Sector has the potential to cause significant cascading impacts to tens, hundreds, or even thousands of other entities. As a result, requiring incident reporting from a broad range of IT Sector entities is essential to developing a complete picture of the cyber threat landscape, identifying vulnerabilities that adversaries are exploiting, and sharing early warnings to better protect entities from across all critical infrastructure sectors.

The IT Sector is comprised of hundreds of thousands of companies, ranging from small businesses to large, multinational enterprises. While some of these companies are likely to be captured by the proposed CIRCIA size-based threshold, many will not be. Additionally, as opposed to many other critical infrastructure sectors with a primary regulatory agency providing oversight or a small number of clearly identifiable subsectors, industry segments, or entity types, the IT sector to a large extent lacks any of these easy means of categorization or segmentation. Given these characteristics, CISA believes it is necessary to take a multi-criteria approach including a general criterion

focused on entities that knowingly provide IT hardware, software, systems, or services to the Federal government, as well as criteria designed to capture critical software, OT, and DNS services that are not used by the Federal government.

For the first IT Sector sector-based criterion, CISA is proposing to include any entity that knowingly provides or supports IT hardware, software, systems, or services to the Federal government either directly or through a reseller. CISA believes this proposed approach will be beneficial in several ways. First, in light of both the essential services provided to the nation by various Federal entities, as well as the symbolic value of the Federal government, Federal entities often are desired targets for attack, and a covered cyber incident impacting a Federal entity can result in significant consequences. Second, because an entity selling a good or service to the Federal government typically will know if it has provided a product or service to the Federal government, the proposed criterion is intended to create a clear and easy manner for an entity within the IT sector to determine if it is a covered entity. This criterion also would include, for example, some entities that provide IT hardware, software, systems, or services to the Federal government through a reseller or by providing software development services, such as a code repository service. It is for this reason CISA proposes capturing in this criterion IT hardware, software, system, or service providers that provide their products to the Federal government only if they knowingly do so, e.g., if they provide goods to the Federal government through a procurement contract or another agreement or transaction. Third, given the breadth of the Federal government and the large number of different IT products and services it employs, CISA expects this criterion to cover a broad spectrum of entities from the IT sector, which will help ensure CISA receives adequate reporting to achieve its responsibilities under CIRCIA as they relate to the IT sector and beyond.

Note, however, while CISA is proposing to use the provision of software, hardware, systems, or services to the Federal government as a criterion for determining who must report, reporting for those entities that meet this sector-based covered entity criteria is not limited to incidents impacting the products or services they provide to the U.S. Government. Rather, an entity that meets this sector-based criteria must report any covered cyber incident it

experiences regardless of whether it impacts any of their Federal customers or the specific products or services used by their Federal customers.

CISA acknowledges that entities routinely change their offerings and customers over time, and that there will be entities who have provided software, hardware, systems, or services to the Federal government at one point but no longer do so (either because they no longer offer or support that software, hardware, system, or service at all, or because their arrangement with their Federal customer(s) has ended). In recognition of this, CISA is proposing that an entity would be captured under this criterion only for as long as the entity continues to sell, provide, or provide support for the product or service they have sold to the government, or any updated versions thereof. If a software, hardware, or system manufacturer or supplier no longer sells or supports the software, hardware, or system that it previously sold to the government, or any updated versions thereof, then it would no longer be considered a covered entity based on this criterion in relation to that particular software, hardware, or system. Similarly, if an IT service provider no longer provides any services to the Federal government, it would not remain a covered entity simply on the basis of having previously provided IT services to the Federal government.

In the second IT sector-based criterion, CISA proposes covering any entity that has developed and continues to sell, license, or maintain any software that meets the definition of “critical software” established by NIST pursuant to Executive Order 14028. On May 12, 2021, President Biden issued Executive Order 14028, with the goal of improving government efforts to identify, deter, protect against, detect, and respond to the persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, private sector, and the American people’s security and privacy. Section 4 of Executive Order 14028 is focused on software supply chain security, with Section 4(g) instructing NIST, in consultation with designated Federal partners, to develop a definition of the term “critical software.” The Federal government would then use the definition of critical software to support the development of a list of software categories and products that would be subject to the additional security activities set forth in the Executive Order, including how the Federal government purchases and manages deployed critical software. In particular,

the Executive Order seeks to limit Federal acquisition to software that has met security measures such as use of a secure development process and integrity checks defined in Section 4(e) of the Executive Order.

To develop the definition of critical software, NIST solicited position papers from the IT community, hosted a virtual workshop to gather input, and consulted with CISA, the Office of Management and Budget (OMB), the Office of the Director of National Intelligence, and the National Security Agency (NSA). Ultimately, NIST defined critical software to be “any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes: (1) is designed to run with elevated privilege or manage privileges; (2) has direct or privileged access to networking or computing resources; (3) is designed to control access to data or operational technology; (4) performs a function critical to trust;²⁷⁷ or, (5) operates outside of normal trust boundaries with privileged access.”²⁷⁸ The definition applies to software of all forms (e.g., standalone software; software integral to specific devices or hardware components; cloud-based software) purchased for, or deployed in, production systems and used for operational purposes.²⁷⁹ Other use cases, such as software solely used for research or testing that is not deployed in production systems, are outside of the scope of this definition.²⁸⁰

Given the purposes for which this definition of critical software was developed (i.e., to support the enhancement of software supply chain security), the informed process that led to its development, and its familiarity to the IT community, CISA believes it to be an appropriate basis for narrowing down the scope of entities engaged in software development for non-Federal government customers included within the description of covered entity. However, because the “critical software” definition has not been formally codified into law or regulation, CISA is proposing to incorporate the

²⁷⁷ According to NIST, the term “critical to trust” covers “categories of software used for security functions such as network control, endpoint security, and network protection.” NIST, *Critical Software Definition—FAQs*, FAQ 3, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-faqs#Ref_FAQ3 (last visited Jan. 26, 2024).

²⁷⁸ See NIST, *Critical Software—Definition & Explanatory Material*, <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory> (last visited July 24, 2023).

²⁷⁹ *Id.*

²⁸⁰ *Id.*

definition of “critical software” developed by NIST directly into the regulatory text rather than by reference, to provide potential covered entities with certainty on the scope of this prong of the IT Sector sector-based criteria.²⁸¹

CISA is also proposing to limit this criterion to entities that continue to sell, license, or maintain critical software. While CISA intends to capture under this criterion entities that continue to be in the business of providing critical software, CISA does not intend to capture former critical software developers in perpetuity if they no longer produce the software. However, to the extent that a critical software developer continues to sell (directly or indirectly), license, or otherwise maintain previously developed critical software, it would continue to be a covered entity under this prong.

For the third IT Sector sector-based criterion, CISA is proposing to include in the description of covered entity any entity that is an OEM, vendor, or integrator of OT hardware or software components. According to NIST,²⁸² OT is defined as “Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples include industrial control systems, building management systems, Fire control systems, and physical access control mechanisms.”²⁸³

OT components are considered vital to the operation of U.S. critical infrastructure, and the security of OT is essential for the achievement of a secure and resilient infrastructure for the American people.²⁸⁴ The increasing convergence of IT and OT creates

²⁸¹ Additional information on the software categories considered to be critical software, the types of products typically included, and the rationale for their inclusion, can be found at <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory> (last visited Nov. 28, 2023).

²⁸² In various places throughout this document, CISA references definitions and guidance found in materials published by NIST. CISA believes it is appropriate to use NIST publications as source references given NIST’s status as a widely recognized and accepted source of cybersecurity information and best practices by and for both industry and government.

²⁸³ NIST, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800–160 Vol. 2 Rev. 1, at 65 (Dec. 2021), available at <https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final>.

²⁸⁴ See *id.* at 1; see also CISA, *Securing Industrial Control Systems: A Unified Initiative—FY 2019–2023*, at 2 (July 2020) (hereinafter, “*Securing Industrial Control Systems*”), available at <https://www.cisa.gov/resources-tools/resources/securing-industrial-control-systems>.

opportunities for exploitation that could result in catastrophic consequences, including loss of life, economic damage, and disruption of the NCFs upon which society relies.²⁸⁵ In light of this, CISA believes it is important to understand the cyberthreat environment related to OT and to receive reports on cyber incidents involving manufacturers or developers of OT products.

OT is typically used in manufacturing and distribution industries, such as electric, water and wastewater, oil and natural gas, chemical, and pharmaceutical manufacturing and distribution. Consequently, the first IT sector-based criterion—focusing on entities that provide hardware, software, systems, or services to the Federal government—may not capture many OT OEMs, vendors, or integrators, resulting in the need for this third criterion.

For the fourth IT Sector sector-based criteria, CISA proposes to include in the description of covered entity certain entities that perform functions related to domain name operations. These are entities whose activities are key to the fabric of the internet, enabling users to access resources on the internet and organizations to provide services online. The criterion is intended to capture entities that perform these functions for the benefit of their customers, business partners, or internet users generally. A successful covered cyber incident perpetuated against such entities could have significant potential consequences not just to the entity itself but also entities across all critical infrastructure sectors that rely upon domain name resolution for their business operations and for the provision of their resources online. In addition, the significance of these entities to enabling navigation of the internet and the potential for compromising one entity in order to impact multiple internet users makes these entities a target for malicious cyber activity. Given their importance to the use of the internet and therefore the potential impacts—to national security, economic security, and public health and safety, as well as to disruption of the reliable operation of critical infrastructure—of a cyber incident perpetrated against such entities, and the attractiveness of such entities to malicious cyber actors, CISA is proposing to include these entities within the definition of covered entities.

CISA believes the inclusion of these four IT sector-based criteria is supported by an analysis of the three factors enumerated in 6 U.S.C. 681b(c)(1) (i.e., consequence, threat, and likelihood of

²⁸⁵ *Securing Industrial Control Systems*, *supra* note 284, at ii.

disruption of the reliable operation of critical infrastructure). First, the disruption to or compromise of any of the entities covered by the proposed criteria for the IT sector has the potential to cause national security, economic security, or public health and safety. This is particularly true for entities that provide or support hardware, software, or services to the Federal government, given the essential role the Federal government has in national security, economic security, and public health and safety. This same rationale is also applicable to entities that develop, license, or sell “critical software”; entities that serve as OEMs, vendors, or integrators of OT; and entities that perform functions related to domain name operations. Critical software and OT frequently are used by entities and systems in a wide variety of critical infrastructure, such as water systems, commercial nuclear power reactors, telecommunications facilities, power grids, airports, and hospitals, that, if disrupted or compromised through the supply chain for these software and technologies, could directly impact national security, economic security, and public health and safety. By definition, critical software operates in a position that provides the software extensive privileges, access, or trust, the compromise of which could be significantly consequential to the systems and networks where they are used, including critical infrastructure systems and networks. OT is used to directly perform a multitude of critical infrastructure functions, such as generating electricity, monitoring and controlling water, and distributing natural gas. As described above, entities that perform functions related to domain name operations play a key role in ensuring the accessibility and security of online services used by entities in a critical infrastructure sector, which may include critical services that depend on those services. For these same reasons, consideration of the third statutory factor—the extent to which damage, disruption, or unauthorized access to such an entity will likely enable the disruption of the reliable operation of critical infrastructure—strongly supports the inclusion of these entities within the description of covered entity. Finally, in terms of the threats targeting the IT sector, these entities have been frequently targeted by malicious cyber actors, which is the second factor identified in 6 U.S.C. 681b(c)(1). The three primary NAICS segments where IT sector entities are found (*i.e.*, the

Manufacturing Sector (for hardware); the Information Sector (for software); and the Professional, Scientific, and Technical Services Sector (for IT services)) routinely rank near the top of the list when it comes to sectors or industries experiencing the most cyber incidents.²⁸⁶

In addition to the four criteria described previously in this section, CISA considered a variety of other potential criteria for inclusion, to include different criteria that would address some of the risks associated with open source code and open source software. Open source software is defined by NIST as “[s]oftware that can be accessed, used, modified, and shared by anyone.”²⁸⁷ Open source code and open source software are, by their very nature, accessible and modifiable by everyone. This means that anyone can identify vulnerabilities, including both good-faith security researchers who report and help fix the vulnerability as well as bad actors who take advantage of their findings to manipulate the software instead of reporting the vulnerability. And while many open source projects are well maintained, resource constraints or limited developer knowledge in some cases lead to vulnerabilities in open source projects. As the practice of integrating open source code with proprietary code and using open source code in downstream software/services has expanded, so has the potential for the incorporation of vulnerabilities into information systems with limited tracking of where the open source software is integrated, making vulnerability management increasingly challenging. With the potential for widespread use or integration of a vulnerable code, and the lack of insight into the full distribution of the code or software in which the code has been integrated, such an inherited vulnerability may be present in millions of instances and difficult to identify potential victims. The potential compromise of a code repository that houses and shares open source code could also lead to largescale downstream effects.

To better understand these threats associated with open source code and open source software, CISA considered including in the description of covered entity any managed service provider or CSP that utilizes open source software

²⁸⁶ See *Verizon 2023 DBIR*, *supra* note 186, at 50; *Verizon 2022 DBIR*, *supra* note 181, at 50; *IBM 2023 Threat Index*, *supra* note 217, at 42.

²⁸⁷ See NIST Suborder 6106.01 Ver. 1, *Open Source Code* at 1 (Dec. 6, 2018), available at <https://www.nist.gov/open/policies-directives-and-nists-public-access-plan>.

within its proprietary software library. CISA also considered including in the description of covered entity specific criteria to cover any code repository platform that hosts open source code or open source software for public use. At this time, CISA has elected not to include specific criteria in the proposed rule, but, as explained earlier, CISA interprets the first proposed IT Sector sector-based criterion to capture software development services, such as a code repositories hosting open source code, that know their services are being used by the Federal government.

CISA is interested in receiving comments on:

19. The scope of entities that would and would not be considered covered entities based on the four unique criteria proposed by CISA, whether the scoping is appropriate, and what, if any, specific refinements should CISA consider related to any of the four criteria.

20. The types of entities that are “related to domain name operations” and what type of relationship such entities may have with relevant multi-stakeholder organizations, such as the internet Corporation for Assigned Names and Numbers. Please also see Section IV.D.ii in this document for additional requests for comment on the proposed DNS Exception.

21. Whether CISA should include in the final rule specific criteria to cover managed service providers or CSPs utilizing open source software or additional, specific criteria that would require reporting related to open source code, open source software, or code repositories.

22. How the proposed IT Sector sector-based criteria might apply to members of the open-source ecosystem, including whether entities that may provide IT hardware, software, systems, or services to the Federal government know or could determine whether they are providing such goods or services to the Federal government, and, if so, the level of effort in making such a determination.

k. Nuclear Reactors, Materials, and Waste Sector

The Nuclear Reactors, Materials, and Waste Sector is composed of nearly 100 commercial nuclear power reactors; over 30 Research and Test Reactors (RTRs); approximately ten fuel cycle facilities; thousands of licensees of radioactive materials for medical, research, and industrial purposes; and the millions of radioactive packages transported yearly.²⁸⁸ Of these entities,

²⁸⁸ See DHS, *Nuclear Reactors, Materials, and Waste SSP: An Annex to the NIPP 2013* (2015),

CISA proposes to include in the description of covered entity any entity that owns or operates a commercial nuclear power reactor or fuel cycle facility. Commercial nuclear power reactors are subject to regulations that require them to report cyber incidents impacting safety, security, or emergency preparedness functions to the NRC; however, other Nuclear Reactors, Materials, and Waste Sector infrastructure typically are not subject to similar cyber incident reporting requirements.

Consideration of the factors enumerated in 6 U.S.C. 681b(c)(1) supports the inclusion of commercial nuclear power reactors and fuel cycle facilities within the description of covered entity. The first factor, which relates to consequence, the disruption or compromise of a commercial nuclear power reactor may present a significant risk to public health, economic security, and national security, as validated by the extensive security regulations imposed by the NRC on these facilities.²⁸⁹ Similarly, in the latest Update to the U.S. NRC Cyber Security Roadmap, the NRC staff stated that the nuclear material and hazardous chemicals at fuel cycle facilities “present safety and security concerns that could lead to potential consequences of concern . . . as a result of a cyber attack.”²⁹⁰

The second factor enumerated in 6 U.S.C. 681b(c)(1) is the likelihood that an entity may be targeted by a malicious cyber actor, including a foreign country. According to the NRC, “[c]yber threats to NRC licensees are dynamic due to emerging technologies and the continuing evolving capabilities of potential adversaries.”²⁹¹ Foreign countries remain interested in perpetrating cyber incidents at U.S. nuclear entities, with DHS recently stating that “Russian government-affiliated cyber espionage likely will remain a persistent threat to . . . entities in the . . . nuclear industry[y].”²⁹²

The third factor enumerated in 6 U.S.C. 681b(c)(1) is the extent to which damage, disruption, or unauthorized access to such an entity is likely to enable the disruption of the reliable operation of critical infrastructure. As

commercial nuclear power reactors themselves are critical infrastructure, damage, disruption, or unauthorized access at a plant likely would result in the disruption of critical infrastructure. Additional infrastructure beyond the commercial nuclear power reactor or fuel cycle facility could also be impacted by a successful cyber incident at one of these entities either through the loss of power provided by the commercial nuclear power reactor or the emission of radiation rendering nearby critical infrastructure generally not safely accessible for some period of time.

In developing this sector-based criteria, CISA also explored including RTRs in the description of a covered entity. However, the security risks associated with RTRs are significantly lower than the risks associated with commercial nuclear power reactors.²⁹³ Based on this lower risk assessment, CISA is not proposing to include a specific Nuclear Sector sector-based criteria capturing RTRs within the description of covered entity. An owner or operator of an RTR nevertheless may be a covered entity based on the size-based threshold or other sector-based criteria, such as the Government Facilities Sector sector-based criteria for the education subsector.

1. Transportation Systems Sector

CISA proposes to include a number of different sector-based criteria for entities in the Transportation Systems Sector. First, CISA is proposing to include criteria related to owners and operators of various non-maritime transportation system infrastructure, such as freight railroad, public transportation and passenger railroads (PTPR), pipeline facilities and systems, over-the-road bus (OTRB) operations, passenger and all-cargo aircraft, indirect air carriers, airports, and Certified Cargo Screening Facilities. Additionally, CISA is proposing to include in the description of covered entity any entity that owns or operates a vessel, facility, or outer continental shelf facility subject to 33 CFR parts 104, 105, or 106.

Transportation is one of four designated lifeline functions, meaning the reliable operation of this function is so critical that a disruption or loss of this function will directly affect the security and resilience of critical infrastructure within and across numerous sectors.²⁹⁴ Transportation

entities have long been targeted by terrorists and other malicious actors, so it is no surprise that as the cyberthreat has evolved, transportation entities are routinely experiencing cyber incidents.²⁹⁵ In light of this evolving and pervasive threat, TSA has identified and imposed heightened cybersecurity requirements on critical entities across the various transportation modes. CISA is proposing to include within the description of covered entity those entities identified by TSA as requiring cyber incident reporting and (in some cases) enhanced cybersecurity measures for primarily the same reasons TSA relied upon in determining that these entities warranted such requirements. Those specific rationales for the proposed inclusion of each of the different Transportation Systems Sector criteria are provided in the following paragraphs. CISA believes that aligning CIRCIA’s Applicability section with the population of entities that TSA requires cyber incident reporting from or the implementation of enhanced cybersecurity measures at is appropriate for CIRCIA and consistent with the factors contained in 6 U.S.C. 681b(c)(1) (*i.e.*, (1) the consequences that a disruption or compromise of one of those entities could cause to national security, economic security, or public health and safety; (2) the likelihood that one of those entities may be targeted by a malicious cyber actor; and (3) the extent to which damage, disruption, or unauthorized access to such an entity will likely enable the disruption of the reliable operation of critical infrastructure). CISA recognizes that some of the criteria proposed below is based on TSA’s Enhancing Surface Cyber Risk Management NPRM, and CISA will continue to coordinate with TSA throughout the rulemaking process to harmonize CIRCIA’s Applicability section with TSA, to the maximum extent practicable.

In the rail subsector, CISA is proposing to require reporting from owners and operators of freight railroad carriers identified under 49 CFR 1580.1(a)(1), (4), and (5) and PTPR identified in 49 CFR 1582.1. This is consistent with the factors contained in 6 U.S.C. 681b(c)(1), as TSA determined these entities should be required to report cyber incidents, with the higher-risk PTPR also warranting enhanced cybersecurity requirements, “due to the ongoing cybersecurity threat to surface transportation systems and associated infrastructure to prevent against the

available at <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-nuclear-2015-508.pdf>.

²⁸⁹ See, e.g., 10 CFR part 73.

²⁹⁰ U.S. NRC, *Update to the U.S. NRC Cyber Security Roadmap*, SECY-17-0034, at 5 (Feb. 28, 2017), available at <https://www.nrc.gov/docs/ML1635/ML16354A282.html>.

²⁹¹ *Id.* at 2.

²⁹² 2024 Homeland Security Threat Assessment, *supra* note 188, at 20.

²⁹³ See *id.*; U.S. NRC, *Backgrounder on RTRs* (2020), available at <https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/research-reactors-bg.html>.

²⁹⁴ See *Guide to Critical Infrastructure Security and Resilience*, *supra* note 198, at 4.

²⁹⁵ See, e.g., *IBM 2023 Threat Index*, *supra* note 217, at 42; *Verizon 2022 DBIR*, *supra* note 181, at 50.

significant harm to the national and economic security of the United States that could result from the ‘degradation, destruction, or malfunction of systems that control this infrastructure.’”²⁹⁶ The scope of applicability for surface transportation is broader than in TSA’s Security Directives, but aligns with TSA’s ongoing rulemaking to codify these requirements that is based on a more long-term and strategic view of risk as applied to these modes as well as the applicability for requirements to report physical security incidents in current 49 CFR 1570.203. This scope includes PTPR and OTRB owner/operators upon whom TSA does not impose enhanced cybersecurity requirements but is seeking to impose cyber incident reporting requirements in their ongoing rulemaking efforts. While TSA has determined it is not necessary at this time to impose requirements to implement more robust cybersecurity measures on certain PTPR and OTRBs, TSA and CISA believe it is important that these entities be required to report cyber incidents when they occur. While the costs of the imposition of robust cybersecurity measures upon these PTPRs and OTRBs may not be justified at this time based on known risks, TSA and CISA believe that the improved understanding of the threat environment to the broader transportation sector that would result from the reporting of substantial cyber incidents experienced by any of these entities outweighs the minimal costs of such reporting requirements. In the case of PTPRs, the additional costs of this requirement would be particularly minimal as all PTPRs already are required to report security incidents to TSA pursuant to 49 CFR 1570.203.

CISA is also proposing to require reporting from owners and operators of the critical pipeline facilities and systems, as identified in 49 CFR part 1586 in TSA’s rulemaking, *Surface Cybersecurity Risk Management*. The scope of applicability includes gas, hazardous liquid, carbon monoxide, and liquefied natural gas pipelines, pipeline systems, and facilities that TSA has determined warrant additional cybersecurity measures to “reduce the risk of operational disruption should the Information and/or Operational

²⁹⁶ See, e.g., TSA Security Directive 1580–21–01 series, *Enhancing Rail Cybersecurity*; TSA Security Directive 1582–21–01 series, *Enhancing Public Transportation and Passenger Railroad Cybersecurity*; TSA Security Directive 1580/82–2021–01 series, *Rail Cybersecurity Mitigation Actions and Testing*. TSA’s Security Directives imposing cybersecurity requirements on surface transportation modes are available at <https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit>.

Technology system of a gas or liquid pipeline be affected by a cybersecurity incident.”²⁹⁷ Following a determination that a pipeline is critical, TSA informs the owners and operators of the pipeline of that determination and the additional cybersecurity requirements that thus apply to it.²⁹⁸ This is similarly consistent with the factors contained in 6 U.S.C. 681b(c)(1) as, to determine which pipelines were critical, TSA considered factors such as the volume of product transported and whether the pipeline serves other critical sectors. Additionally, malicious cyber actors continue to target this industry, with the 2023 Verizon DBIR noting nearly 150 cyber incidents for the mining, quarrying, and oil and gas extraction and utilities segment during the year covered by the report.²⁹⁹

Additionally, CISA is proposing to include in the description of covered entity any entity that is required to implement a TSA-approved security program under 49 CFR parts 1542, 1544, 1548, and 1549. This requirement applies to airports, passenger and all-cargo aircraft operators, indirect air carriers, and Certified Cargo Screening Facilities, respectively. In November 2021, TSA issued security program changes requiring these entities to report cybersecurity incidents to CISA. A subset of these entities were subsequently required to implement additional cybersecurity measures in what TSA described as “the latest in TSA’s efforts to require that critical transportation sector operators continue to enhance their ability to defend against cybersecurity threats.”³⁰⁰ As specifically applied to all-cargo aircraft operators, the air cargo system faces emerging risks, including a proliferation of cyber threats.³⁰¹ Adversaries continue to threaten the air cargo system and seek to use the aviation domain to carry out terrorist plots, including through the use of the air cargo supply chain to ship

²⁹⁷ See, e.g., TSA Security Directive Pipeline-2021–01 series, *Enhancing Pipeline Cybersecurity* and TSA Security Directive Pipeline-2021–02 series, *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing*, available at <https://www.tsa.gov/sd-and-ea>.

²⁹⁸ Of note, this means that, for at least this prong of the Transportation Systems Sector sector-based criteria, entities will clearly know that they are covered entities.

²⁹⁹ Verizon 2023 DBIR, *supra* note 186, at 59.

³⁰⁰ TSA Press Release, *TSA Issues New Cybersecurity Requirements for Airport and Aircraft Operators* (Mar. 7, 2023), available at <https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft> (hereinafter “TSA Press Release”).

³⁰¹ TSA, *Air Cargo Security Roadmap* (Dec. 2021), available at <https://www.tsa.gov/news/press/releases/2021/12/09/tsa-publishes-new-roadmap-address-vision-improving-air-cargo>.

dangerous and potentially deadly items for pre-operational planning.³⁰² The focus on these “critical transportation sector operators” in light of the “persistent cybersecurity threats against U.S. critical infrastructure, including the aviation sector”³⁰³ is consistent with the three factors enumerated in 6 U.S.C. 681b(c)(1).

Most, if not all, of the entities that would be captured under these criteria already are required to report cybersecurity incidents to CISA pursuant to these requirements. Including these entities within the description of covered entity would further align the CIRCIA requirements with TSA’s requirements to support reducing duplication and avoid unintended gaps in reporting. For example, while this approach technically creates two legal requirements for these entities to report cyber incidents, CISA does not believe that this is likely to result in any actual duplicative reporting because TSA’s existing requirement requires these entities to report to CISA. CISA is committed to working with TSA to ensure that Transportation Services Sector entities that are required to report to CISA under both CIRCIA and a separate TSA authority can do so in a single report where legally possible. If necessary to do so, CISA and TSA will explore leveraging the substantially similar reporting exception to formalize the ability to comply with CIRCIA and TSA cyber incident reporting requirements through the submission of a single cyber incident report. Additional information on the substantially similar reporting exception can be found in Section IV.D.i in this document.

With the final Transportation Systems Sector sector-based criterion, CISA is proposing to cover those entities that own or operate assets subject to MTSA. MTSA, which is designed to protect the nation’s ports and waterways from a terrorist attack, requires certain vessels, facilities, and outer continental shelf facilities to perform various security-related activities. The goal of MTSA is to prevent a transportation security incident, which is defined as an incident that results in significant loss of life, environmental damage, transportation system disruption, or economic disruption to a particular area.³⁰⁴ This goal is consistent with the first and third factors enumerated in 6

³⁰² See *id.*

³⁰³ TSA Press Release, *supra* note 300.

³⁰⁴ See U.S. Coast Guard, *Operations Home—ISPS/MTSA*, <https://www.dco.uscg.mil/ISPS-MTSA/> (last visited Nov. 28, 2023); 33 CFR 101.100.

U.S.C. 681b(c)(1)—*i.e.*, the consequences that disruption to or compromise of an entity could cause to national security, economic security, or public health and safety, and the extent damage or disruption to an entity will likely enable the disruption of the reliable operation of critical infrastructure. Including MTSA-regulated facilities is also consistent with the second factor enumerated in 6 U.S.C. 681b(c)(1)—the likelihood that an entity may be targeted by a malicious cyber actor, including a foreign country—given the recent assessment in the 2024 Homeland Security Threat Assessment identifying an increased risk from Chinese government cyber actors to target ports for disruption.³⁰⁵ The MTSA-regulated population is generally considered to include all critical maritime assets. Considering that, CISA, after consultation with the USCG, the SRMA for the Transportation Systems Sector Maritime Subsector and regulatory agency responsible for MTSA, believes that entities that own or operate vessels, facilities, or outer continental shelf facilities subject to MTSA should be required to report cyber incidents under CIRCIA. To achieve that, CISA proposes that the description of covered entity include any entity that owns or operates a vessel, facility, or outer continental shelf facility subject to 33 CFR parts 104, 105, or 106.

CISA and USCG recognize that this proposed approach will result in two separate cyber incident reporting requirements for entities that are subject to both MTSA and CIRCIA. CISA and USCG are committed to exploring the substantially similar reporting exception or other mechanisms to allow entities that are subject to both MTSA and CIRCIA cyber incident reporting requirements to comply with both requirements through the submission of a single cyber incident report. Additional information on the substantially similar reporting exception can be found in Section IV.D.i in this document.

m. Water and Wastewater Systems Sector

CISA proposes including within the description of covered entity any entity that owns or operates a Community Water System, as defined in 42 U.S.C. 300f(15), or a Publicly Owned Treatment Works (POTWs), as defined in 40 CFR 403.3(q), that serve more than 3,300 people. Inclusion of water and wastewater systems in the description of

covered entity is supported by a review of how the three factors enumerated in 6 U.S.C. 681b(c)(1) apply to these entities. First, as noted in the 2015 Water and Wastewater Systems SSP, safe drinking water is essential to public health and all human activity, and properly treated wastewater is vital for preventing disease and protecting the environment.³⁰⁶ According to the EPA, “[t]he collection and treatment of . . . wastewater is vital to public health and clean water.”³⁰⁷ The 2015 Water and Wastewater Systems SSP further notes that drinking water and wastewater treatment are essential to modern life and the Nation’s economy.³⁰⁸ Second, as noted in a March 3, 2023 memorandum issued by the EPA related to public water system cybersecurity, water systems are increasingly facing cyberattacks.³⁰⁹ This assessment is supported by the Cyberspace Solarium Commission, which stated in its March 2020 report that the “water supply is known to be a target for malign actors.”³¹⁰ Third, other critical services, such as fire protection, healthcare, and heating and cooling, are dependent on, and would be disrupted by, the interruption or cessation of drinking water services.³¹¹ This criticality to other sectors is reinforced by water having been designated one of four designated lifeline functions, indicating that the sector’s reliable operation is so critical that a disruption or loss of this function will directly affect the security and resilience of critical infrastructure within and across numerous sectors.³¹²

No cyber incident reporting requirements currently exist for water and wastewater infrastructure, creating a significant gap in understanding of the cyber threats to and visibility into emerging TTPs used against water and wastewater infrastructure. This proposed sector-based criterion is intended to close this gap and provide the Federal government with sufficient reporting to better understand the Water

and Wastewater Systems Sector’s cyber threat environment.

In developing this sector-based criterion, CISA considered whether a minimum size threshold, such as population served, should be included in the criterion. Following consultations with the EPA, the SRMA for this sector, CISA has determined that the proposed criterion should only include Community Water Systems and POTWs that serve populations of more than 3,300 people. In regards to Community Water Systems, this threshold, which has been used as the line of demarcation to distinguish small and very small water systems from medium, large, and very large water systems,³¹³ is the threshold for the risk and resilience assessment requirements established by Congress in 42 U.S.C. 300i–2(a)(1).³¹⁴ Section 300i–2(a)(1) and (b) of title 42 of the United States Code requires Community Water Systems serving a population of more than 3,300 people to conduct risk and resilience assessments and to prepare an emergency response plans that incorporate the findings of the assessments performed.³¹⁵ CISA interprets Congress’s decision to limit the 42 U.S.C. 300i–2(a)(1) risk and resilience assessment requirements to facilities serving more than 3,300 individuals as an indication of Congress’s assessment of the relative risk associated with these facilities, and CISA agrees with this assessment for the reasons stated above. This interpretation is consistent with the fact that, generally speaking, Community Water Systems that serve larger populations will de facto present greater potential risks to public health and safety, if compromised, in light of the significantly larger populations that rely on their water service. Similar logic supports the application of the 3,300-population-served threshold for POTWs, as does the rationale discussed in Section IV.B.iv.1.a for the proposed inclusion of larger entities in the covered entity population. By setting the threshold for coverage of water and wastewater treatment systems at a population served of more than 3,300 individuals, this criterion would be limiting required reporting to approximately the largest 20% of water

³⁰⁶ See DHS, *Water and Wastewater Systems SSP* at 1 (2015), available at <https://www.cisa.gov/2015-sector-specific-plans> (hereinafter “*Water and Wastewater Systems SSP*”).

³⁰⁷ See EPA, *Municipal Wastewater*, <https://www.epa.gov/npdes/municipal-wastewater> (last visited Nov. 28, 2023).

³⁰⁸ *Water and Wastewater Systems SSP*, *supra* note 306, at i.

³⁰⁹ Assistant Administrator Fox, *Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process* (Mar. 3, 2023), available at <https://www.epa.gov/waterresilience/cybersecurity-sanitary-surveys>.

³¹⁰ *Cyberspace Solarium Commission Report*, *supra* note 23, at 62.

³¹¹ See *Water and Wastewater Systems SSP*, *supra* note 306, at 2.

³¹² See *Guide to Critical Infrastructure Security and Resilience*, *supra* note 198, at 4.

³¹³ See, e.g., *Water and Wastewater Systems SSP*, *supra* note 306, at 3.

³¹⁴ 42 U.S.C. 300i–2(a)(1).

³¹⁵ See *id.*; see also EPA, *America’s Water Infrastructure Act Section 2013: Risk and Resilience Assessments and Emergency Response Plans*, <https://www.epa.gov/waterresilience/awia-section-2013> (last visited Nov. 28, 2023).

³⁰⁵ 2024 *Homeland Security Threat Assessment*, *supra* note 188, at 20.

and wastewater treatment systems by population served.³¹⁶

In establishing this proposed criterion, CISA, in consultation with EPA, did consider not including a size threshold and instead requiring reporting from all water systems and POTWs. CISA believes that including all water systems and POTWs as a criteria is a reasonable alternative. A cyber incident that results in a compromise of water treatment even for smaller communities arguably is a significant enough potential public health concern that it should warrant reporting to the Federal government. Moreover, because this sector is predominantly composed of smaller entities, reporting of incidents from smaller entities in this sector could be essential to CISA receiving a sufficient volume of reports to identify trends, TTPs, and vulnerabilities that can be used to provide early warnings to water and wastewater facilities of all sizes. Cutting against the argument to include all water and wastewater systems in the covered entity definition is the fact that many of the smallest water systems and POTWs, such as hand pump operated wells at a campground or other small facility, do not currently utilize information systems, and thus, could not be the target of malicious cyber activity or experience a covered cyber incident. Additionally, given that there are more than 150,000 combined Public Water Systems (which includes both Community Water Systems and non-community water systems) and POTWs, were CISA to include all of those entities in the description of covered entity, it would dramatically increase the scope and burden of the proposed regulations, with water and wastewater facilities accounting for nearly 40% of all covered entities.

After weighing these considerations, CISA ultimately concluded that proposing limiting reporting required by CIRCIA to medium, large, and very large Community Water Systems and POTWs entities is the optimal approach. CISA would be interested in comments on:

23. The proposed Water and Wastewater Systems Sector sector-based criterion.

24. The alternative criterion for the Water and Wastewater Systems Sector that was considered.

n. Sectors for Which CISA Is Not Proposing Any Sector-Based Criteria

CISA is not proposing any sector-based criteria for three sectors: the Commercial Facilities Sector, the Dams

Sector, and the Food and Agriculture Sector. CISA's rationale for proposing to not include sector-based criteria for each of these sectors is described below. Instead, CISA proposes to rely on the Applicability section's size-based criterion or other sector-based criteria to capture the largest entities in these critical infrastructure sectors for the reasons described below.

The Commercial Facilities Sector is made up of an extremely diverse range of physical and virtual sites where large numbers of people congregate to conduct business, purchase retail products, and enjoy recreational events and accommodations. It is divided into eight subsectors—Entertainment and Media, Gaming, Lodging, Outdoor Events, Public Assembly, Real Estate, Retail, and Sports Leagues. While members of certain subsectors are at higher risk of cyber incidents, such as the Entertainment and Media, Gaming, and Lodging subsectors, the results of a cyber incident impacting an individual small entity in those industries are unlikely to affect national security, economic security, or public health and safety. To the extent that a Commercial Facilities entity is large enough where there is the potential that a cyber incident affecting it could result in impacts to national security, economic security, or public health and safety, CISA believes it likely the entity would be captured by the Applicability section's size-based criterion. As a result, CISA is not proposing a sector-based criteria for the Commercial Facilities Sector.

The Dams Sector consists of, among other things, over 100,000 dams, an estimated 100,000 miles of levees, nearly 250 locks, and 150,000 mine tailings. The majority of these do not have integrated information systems and thus do not warrant coverage under the CIRCIA regulations at this time. Those assets that do have significant integrated information systems, such as large dams, hydroelectric power dams, and locks, frequently are owned by Federal entities or, in the case of certain hydroelectric or other dams, are likely to be covered entities under the proposed Energy Sector or Water and Wastewater Systems Sector sector-based criteria. CISA, therefore, is not proposing a sector-based criteria for the Dams Sector.

The Food and Agriculture Sector covers a broad landscape of entities, including more than 2 million farms; nearly 1 million restaurants; over 100,000 supermarkets, grocery stores, and other food outlets; and thousands of meat, poultry, egg, and imported food processors, warehouse, and

distributors. Based on consultations with the FDA and the U.S. Department of Agriculture (USDA), who serve as co-SRMAs for this sector, CISA believes that given the scale of this sector and the general substitutability of the products that entities within the sector produce, the Food and Agriculture Sector entities with the greatest potential to experience a cyber incident resulting in significant consequences are the largest entities in this sector. For this reason, FDA regulations focused on food defense incorporate a size-based threshold, applying more stringent regulatory requirements to the largest entities.³¹⁷ Based on this, and after consultation with the FDA and USDA, CISA believes that the size standard proposed by CIRCIA will capture a sufficient number of Food and Agriculture Sector entities, including the most critical Food and Agriculture Sector entities, within the description of covered entity, and that additional Food and Agriculture Sector sector-based criteria are unnecessary for the purposes of CIRCIA.

CISA believes that it can rely on other criteria for adequate reporting from these three sectors. However, if as a result of public comment CISA determines that it must modify or eliminate any aspect of the Applicability section's description of a covered entity such that coverage of these three sectors is no longer deemed adequate, CISA may incorporate sector-based criteria for these three sectors in the final rule.

For the Commercial Facilities sector, CISA is relying on the proposed size-based threshold criterion for reporting. Were that criterion to be modified or eliminated prior to the issuance of the final rule, one alternative sector-based criterion CISA likely would consider would be to capture certain sector

³¹⁷ See *Mitigation Strategies To Protect Food Against Intentional Adulteration*, 21 CFR part 121. As FDA explained in the NPRM for those regulations, "[The FDA assesses] that the goal of terrorist organizations is to maximize public health harm and, to a lesser extent, economic disruption. It is our assessment that such goals are likely to drive terrorist organizations to target the product of relatively large facilities, especially those for which the brand is nationally or internationally recognizable. An attack on such a target would potentially provide the wide-scale consequences desired by a terrorist organization and the significant public attention that would accompany an attack on a recognizable brand. Such facilities are likely to have larger batch sizes, potentially resulting in greater human morbidity and mortality. Further, an attack on a well-recognized, trusted brand is likely to result in greater loss of consumer confidence in the food supply and in the government's ability to ensure its safety and, consequently, cause greater economic disruption than a relatively unknown brand that is distributed regionally." 78 FR 78033.

³¹⁶ See *Water and Wastewater Systems SSP*, *supra* note 306, at 3, 6.

entities that exceed one or more designated annual revenue or number of employees thresholds. This could be structured as a single threshold for all Commercial Facilities Sector entities, or it could vary based on subsectors or industry segments. If a single threshold were to be used for all entities in the sector, CISA likely would use the SBA Size Standards to inform that decision and develop a possible average threshold, but would not use the SBA Size Standards alone since the applicable size thresholds in the SBA Size Standards for Commercial Facilities Sector entities vary depending on the type of entity and associated NAICS code. An alternative approach to developing a single size threshold for the sector-based criterion for this sector would be to simply use the SBA Size Standards themselves (*i.e.*, an entity in the Commercial Facilities sector that exceeds the applicable SBA Size Standard), which is how entities in this sector would be considered covered entities under the current proposal. In either case, CISA would attempt to set any threshold to cover the same larger entities in the sector which would be required to report under the proposed size-based criterion.

Coverage of entities in the Food and Agriculture Sector in the current proposed approach similarly is reliant on the size-based threshold criterion. If as a result of public comment CISA determines that it must eliminate or modify the size-based criterion, CISA likely would propose multiple different Food and Agriculture Sector sector-based criteria to ensure that these entities remain covered entities. This is likely to include one criterion targeting larger food manufacturers, processors, warehouses, and similar entities; one criterion targeting larger food producers (*e.g.*, farms, orchards, groves, ranches, hatcheries, fisheries); and one criterion larger targeting groceries, supermarkets, and other food outlets. For food manufacturers, processors, warehouses, and similar entities, a potential approach to developing this criterion would be to mirror the approach used in the Food Safety Modernization Act's International Adulteration rule (21 CFR part 121), which regulates food manufacturers, processors, warehouses, and similar entities that have more than 500 employees. For food producers, CISA could leverage the SBA size standards table to set a size threshold for this criterion based on annual revenue. As the SBA Size Standards use slightly different revenue thresholds for different types of food producers, CISA could elect to use the mean, median, or

mode of the different revenue amounts used in this industry segment or simply have entities refer to the applicable size standard for their industry in the SBA Size Standards table. For the final group, *i.e.*, supermarkets, groceries, and other food outlets, CISA could use a similar approach to set a size threshold for this criterion, except for these types of entities, the SBA Size Standards tend to use number of employees as opposed to annual revenue to distinguish between small and large entities. Thus, this criterion is likely to be a size threshold based on the mean, median, or mode of number of employees across such entities.

As noted above, the only Dams Sector assets that are likely to have integrated information systems warranting coverage under CIRCIA are large dams, hydroelectric power dams, and locks. With the Federal government responsible for 80% of the largest dams and all navigation locks,³¹⁸ the only segment of this sector where CISA might not have insight into incidents without CIRCIA reporting would be the 2,600 non-Federal hydroelectric dams. Unlike the Commercial Facilities and Food and Agriculture Sector entities, CISA is currently not proposing a separate standard for this sector because CISA believes these entities are sufficiently covered in the proposed covered entity description not by the size-based criterion, but by other sector-based criteria, namely the Energy Sector sector-based criterion and, to a lesser extent, the Water and Wastewater Systems Sector sector-based criterion. Accordingly, if as a result of public comment CISA determines that it must modify or eliminate the proposed size-based criterion from the final rule, but the proposed Energy Sector sector-based criterion remained, CISA does not believe it would need to propose a separate Dams Sector sector-based criterion. If, however, either the Energy Sector or Water and Wastewater Systems Sector sector-based criterion were modified or eliminated as a result of public comment, CISA may need to add a Dams Sector sector-based criterion to the final rule to ensure reporting from appropriate non-Federal hydroelectric dams. In such a case, CISA would consult with FERC and the Dams SRMA to identify an appropriate criterion for this industry segment. A possible alternative criterion could be based on energy generating capacity.

³¹⁸ See *Dams SSP: An Annex to the NIPP 2013* at v (2015), available at <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-dams-2015-508.pdf>.

CISA is interested in receiving comments on:

25. The proposed approach to the Commercial Facilities Sector, Dams Sector, and Food and Agriculture Sector.

26. Potential alternative sector-based criteria for each of those three sectors if CISA modifies or removes the general size-based threshold criterion, the Energy Sector sector-based criterion, or the Water and Wastewater Systems Sector sector-based criterion in the final rule.

o. Interpretation of Sector-Based Criteria Coverage

When an entity is assessing whether it is a covered entity based on any of the sector-based criteria, the entity should not factor into its assessment the critical infrastructure sector of which the entity considers itself to be a part. By definition, each of the sector-based criterion include entities that are in a critical infrastructure sector, and entities should therefore assume they meet this threshold requirement of being "in a critical infrastructure sector" if they meet one or more sector-based criteria, without needing to undertake any determination described in Section IV.B.ii, above. CISA will determine whether an entity is a covered entity based on whether the entity meets any of the specified criteria in § 226.2 of the proposed rule. Whether or not the entity considers itself part of the specific critical infrastructure sector that the sector-based criteria targets or is based upon is irrelevant for the purposes of determining whether the entity is a covered entity. For example, if a pharmaceutical manufacturer owns a covered chemical facility subject to CFATS (or, if CFATS is not reauthorized by the publication of the final rule, the EPA RMP), it would qualify as a covered entity regardless of whether or not the pharmaceutical manufacturer considers itself part of the Chemical Sector. Similarly, if an SLTT Government entity owns or operates a Community Water System as defined in 42 U.S.C. 300f(15), it would qualify as a covered entity regardless of its Title IV status even if it considers itself a member of the Government Facilities Sector, and not the Water and Wastewater Systems Sector. Thus, an entity may qualify as a covered entity under a sector-based criterion for a sector with which it does not typically identify, and an entity may qualify as a covered entity under two different sector-based criteria. However, an entity only needs to meet one of the sector-based criteria proposed in the Applicability section to qualify as a covered entity.

As noted throughout this section, CISA recognizes that a number of the entities that are captured under the Applicability section already are, or in the future will be, required to report cyber incidents to a different Federal department or agency pursuant to another existing or proposed regulation. CISA could have attempted to design the sector-based criteria in a manner to avoid designating entities that may be subject to other Federal cyber incident reporting requirements as covered entities. With one exception, however, CISA has no authority over those other regulations.³¹⁹ If CISA were to carve those entities out of CIRCIA's Applicability section, CISA would have no control over what incidents the entities must report or what information must be included in those reports.³²⁰ CISA also would be unable to guarantee it would receive such reports in a timely manner. To ensure that CISA continues to receive reports from entities containing the information needed to support the CIRCIA mission in a manner and timeframe that support CIRCIA implementation, CISA proposes not to use other existing regulatory coverage as a disqualifying factor for inclusion within the description of covered entity. As noted earlier, CISA is committed to working with its Federal partners to explore the implementation of the substantially similar reporting exception where practicable to minimize duplicative reporting. Moreover, this approach is consistent with Congressional intent behind the CIRCIA legislation, which included providing CISA, as the newly minted central repository for cyber incident reporting, visibility into significant cyber incidents being conducted across U.S. critical infrastructure sectors and enabling coordinated, informed Federal government action against perpetrators of cyberattacks.³²¹

³¹⁹ CISA is responsible for implementation of the CFATS, 6 CFR part 27, which requires CFATS-covered chemical facilities to report certain cyber incidents to CISA, although CISA acknowledges that at the time of publication of this NPRM, Congress has allowed the statutory authority for CFATS to lapse.

³²⁰ CISA recognizes that CISA proposes to use regulations that CISA does not administer to help scope what entities meet the CIRCIA Applicability. If following the publication of a final rule implementing CIRCIA the population covered by those other regulations changes, CISA will review the change and may seek to update the CIRCIA regulations if the existing regulatory citation no longer reflects the population from which CISA seeks to receive reporting under CIRCIA.

³²¹ See, e.g., *HSGAC Fact Sheet*, *supra* note 2, at 1 (“Today no one U.S. Government agency has visibility into all cyber-attacks occurring against U.S. critical infrastructure on a daily basis. This bill would change that—enabling a coordinated, informed U.S. response to the foreign governments

v. Other Approaches Considered To Describe Covered Entity

In addition to the proposed approach, CISA considered various other options for how to describe covered entity. Among other approaches, CISA considered simply using the statutory definition contained in CIRCIA (*i.e.*, any entity in a critical infrastructure sector); aligning the Applicability section to an existing definition of “critical infrastructure;” and describing covered entity as the entities identified pursuant to Section 9 of Executive Order 13636—Improving Critical Infrastructure Cybersecurity (78 FR 11737). CISA opted against using any of these approaches either as a standalone approach or, where it would not make the other prongs redundant, as a third prong to the proposed approach for the reasons described below.

1. Alternative A: Any Entity in a Critical Infrastructure Sector

One alternative approach CISA considered for describing covered entity was to scope the term as broadly as permissible under the statute—*i.e.*, to include “any entity in a critical infrastructure sector, as defined in PPD-21.” As discussed earlier, while the term “critical infrastructure sector” is not defined in PPD-21, public and private sector partners for each of the critical infrastructure sectors identified in PPD-21 jointly developed SSPs for their respective sectors that set out goals and priorities for the sector to address its current risk environment.³²² Each of those SSPs includes a description of the entities that compose the sector in Sector Profiles. As the examples provided earlier demonstrate, most of these sectors are quite expansive, and entities “in a critical infrastructure sector” are not limited to—and are often broader than—entities that own or operate systems or assets that meet the statutory definition of “critical infrastructure.” See Section IV.B.ii in this document. Based on a consolidated reading of these sector-developed descriptions in the various SSP Sector Profiles, CISA believes that the overwhelming majority of entities in the United States—though not all—fit within one or more of the critical infrastructure sectors and thus would meet the definition of “an entity in a critical infrastructure sector.”

According to Census Bureau records, there are more than 8 million employers

and criminal organizations conducting these attacks against the U.S.”).

³²² See CISA, *2015 Sector Specific Plans*, available <https://www.cisa.gov/2015-sector-specific-plans> (last visited Nov. 28, 2023).

in the United States and another approximately 27 million legal establishments that do not have any employees.³²³ Combined, that would indicate the existence of approximately 35 million entities with legal standing within the United States. Given that very few types of entities are not part of one of the 16 critical infrastructure sectors, CISA believes that the vast majority of these 35 million entities would qualify as an “entity in a critical infrastructure sector.”

Although CISA anticipates the per-report cost of this regulation to be relatively low, the aggregate cost of reportable incidents across tens of millions of entities has the potential to be extremely large and burdensome. Additionally, while CISA believes receiving a large number of reports is necessary to achieve the goals of the CIRCIA regulation, CISA acknowledges that there likely is some point at which the marginal returns provided by each additional report will be outweighed by the cost of its submission. Although it is difficult to pinpoint with precision that point of diminishing marginal returns, CISA is confident that it would be surpassed were CISA to require reporting from tens of millions of entities.

2. Alternative B: Removal of Size-Based Threshold

A second alternative CISA considered was to use the same general framework as in the current proposed approach, but without the size-based criterion. Under this approach, CISA would only rely upon sector-based criteria to cover the desired population of entities in each critical infrastructure sector. As the existing sector-based criteria do not cover all of the sectors and subsectors from which CISA believes reporting is necessary, were CISA to eliminate the size-based criterion, CISA would have to propose adding new sector-based criteria to ensure appropriate coverage of covered entities. Sectors or subsectors for which CISA would need to add new sector-based criteria include the Commercial Facilities Sector, the Dams Sector, the Food and Agriculture Sector, certain parts of the Healthcare and Public Health Sector (*e.g.*, medical insurers; laboratories and other diagnostic facilities), and the Oil and Natural Gas Subsector.

³²³ See, e.g., U.S. Census Bureau, *County Business Patterns First Look Report for 2021*, available at <https://www.census.gov/data/tables/2021/econ/cbp/2021-first-look.html>; U.S. Census Bureau, *Nonemployer Statistics Tables for 2019*, available at <https://www.census.gov/programs-surveys/nonemployer-statistics/data/tables.html>.

Removing the size-based criterion and replacing it with some number of new sector-based criteria would have two primary effects. First, the total number of covered entities likely would be slightly reduced as there are some entities currently captured by the size-based criterion that would not meet any of the current proposed or potential additional sector-based criteria. CISA believes that such entities would be relatively few, however, as CISA estimates that the majority of entities that currently meet the size-based criterion either also meet one of the current sector-based criteria or would be brought into the covered entity definition by a new sector-based criterion.

Second, CISA believes that this alternative could slightly reduce familiarization costs associated with the regulation, as entities that would have had to expend resources to determine if they exceeded the SBA Size Standard for their respective industry no longer would have to do so. CISA believes that this impact would also be fairly limited as: (a) only a portion of potentially covered entities would need to expend resources to make such a determination since many already know if they exceed the small business size standard for their respective industry, (b) the amount of resources necessary to do so typically are relatively minimal, and (c) a portion of the resources certain entities would save by the elimination of the size-based criterion would instead be expended by those or other entities to determine if they meet one of the new sector-based criteria.

Contrary to the minimum benefits likely to be gained by elimination of the size-based criterion, CISA believes there are significant reasons to include the criterion in the proposal. First, as described at length in Section IV.B.iv.1 above, there are a number of reasons why CISA believes requiring reporting from large entities is beneficial. Second, the size-based criterion allows CISA to capture adequate reporting populations from multiple sectors and subsectors using a single threshold. As noted above, without the size-based criterion, CISA would need to establish one or more new sector-based criteria for each of at least five critical infrastructure sectors or subsectors. In total, while CISA believes it could achieve the purposes of the CIRCIA statute without a size-based criterion, CISA believes that the benefits of including the size-based criterion far exceed the almost certainly minimal cost savings associated with an alternative where additional sector-based criteria are used in lieu of the size-based criterion.

3. Alternative C: Definition of Critical Infrastructure

CISA also explored potentially limiting the scope of the covered entity description to critical infrastructure only and using an existing definition of critical infrastructure, such as the one at 42 U.S.C. 5195c(e).³²⁴ As discussed earlier, however, CISA believes that such a narrow scope of applicability would severely limit, and perhaps prevent, CISA's ability to achieve CIRCIA's regulatory purposes. See Section III.C.ii. Additionally, the 42 U.S.C. 5195c(e) definition of "critical infrastructure" includes some ambiguity that can make it difficult for certain entities to know definitively whether they meet the definition. For example, it is not readily apparent what level of impact would constitute a "debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."³²⁵ Moreover, even if a clear definition of that level of impact existed, it would be unreasonable to expect most private sector entities to be able to determine if an incident impacting one of their systems would have a debilitating impact on national security, national economic security, national public health or safety, or any combination thereof. Because the description of covered entity will impose regulatory requirements on entities, it is important that the description be easily understandable and allow different individuals interpreting the description to routinely come to the same conclusion.

4. Alternative D: Section 9 List

In comments submitted in response to the RFI, a number of commenters recommended that CISA use the list of entities developed pursuant to Section 9(a) of Executive Order 13636 (hereinafter referred to as the Section 9 List) as either a starting point for identifying, or the complete list of, covered entities.³²⁶ The Section 9 List contains "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national

security."³²⁷ Pursuant to Executive Order 13636, DHS is to review and update this list annually.

Given that the Section 9 List consists of entities against which a cybersecurity incident could result in catastrophic effects on national security, economic security, or public health, CISA agrees that the entities on the Section 9 List are entities that CISA would want to report covered cyber incidents and ransom payments under CIRCIA. CISA anticipates, however, that all of the entities on the Section 9 List would be covered entities under either the proposed size-based criterion or sector-based criteria in the proposed Applicability section, rendering any benefits of using the Section 9 List as a basis for coverage under CIRCIA extremely limited. CISA further believes that the limited benefits of potentially requiring reporting from a few Section 9 List entities who would not already be required to report under other proposed criteria are outweighed by the significant potential downsides associated with using the Section 9 List in this manner.

First, CISA is concerned that using the Section 9 List, which relies in part on nominations to identify entities for inclusion, as the basis for imposing regulatory requirements would chill nominations to the list and reduce voluntary participation in cybersecurity efforts targeted at Section 9 List entities. Depending on how much the use of the Section 9 List for regulatory purposes disincentivizes cooperation in the development of the list and participation in voluntary cybersecurity activities targeted at Section 9 List entities, using the list for CIRCIA could result in a net overall negative impact to national cybersecurity efforts.

Second, because of the requirement that CISA update the list annually, entities would lack certainty regarding their future regulatory status under CIRCIA. This would not only be frustrating to entities, but it could also result in some entities wasting resources to establish regulatory reporting processes and procedures that they end up not needing or, conversely, result in some entities foregoing establishing reporting processes and procedures with the thought that they might not be subject to regulatory requirements the following year. The annual updates to the list would also present logistical challenges for CISA, which would need to inform entities whenever they are

³²⁴ 42 U.S.C. 5195c(e) defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

³²⁵ *Id.*

³²⁶ See, e.g., Comments submitted by UnityPoint Health, CISA-2022-0010-0107; National Retail Federation, CISA-2022-0010-0092; National Rural Electric Cooperative Association, CISA-2022-0010-0025.

³²⁷ E.O. 13636 Section 9(a), available at <https://www.cisa.gov/resources-tools/resources/executive-order-13636-improving-critical-infrastructure-cybersecurity>.

added to, or removed from, the list for the entities to be aware of their regulatory status.

vi. Request for Comments on Applicability Section

CISA seeks comments on all aspects of the Applicability Section, to include comments on the following specific topics:

27. CISA's interpretation of the terms "entity" and "in a critical infrastructure sector."

28. Potential challenges for an entity determining whether it is "in a critical infrastructure sector" and any specific changes that can be made to the proposed § 226.2 (Applicability) that would provide additional clarity for an entity to make this determination.

29. The scope of entities that would only be considered covered entities because of the size-based criterion and would not meet any of the sector-based criteria.

30. The use of both a size-based criterion and sector-based criteria as criteria in the description of covered entity.

31. The proposed decision to include a size-based criterion.

32. The proposal to use the SBA Size Standards as the basis for the size-based criterion and the Small Business Size Regulations instructions for determining if an entity exceeds the size threshold for purposes of determining applicability of these regulations to certain entities.

33. The proposed sector-based criteria used in the Applicability Section to identify certain entities as covered entities.

34. Any additional sector-based criteria that would be necessary to capture entities who are only considered covered entities because of the size-based criterion if the size-based criterion was removed the Final Rule.

35. The use of the EPA RMP rule as an alternative Chemical Sector sector-based criteria should CFATS not be reauthorized at the time of the issuance of the CIRCIA final rule.

36. The proposed decision to forgo inclusion of sector-based criteria for certain critical infrastructure sectors, subsectors, industries, or entity types, and the alternative proposed criteria for those sectors, subsectors, industries, and entity types.

37. Whether there are other lists of entities in a critical infrastructure sector that should be included as covered entities (either instead of the applicability criteria for covered entity proposed in this NPRM or in addition to the proposed applicability criteria), to

the extent that those listed entities fall within a critical infrastructure sector.

C. Required Reporting on Covered Cyber Incidents and Ransom Payments

i. Overview of Reporting Requirements

Pursuant to 6 U.S.C. 681b(a)(1)–(3), four proposed circumstances exist that require covered entities (or third parties on their behalf) to submit a report to CISA, subject to certain proposed exceptions or limitations discussed in Sections IV.D and IV.E.ii of this document. First, CIRCIA requires a covered entity that experiences a covered cyber incident to report that incident to CISA. 6 U.S.C. 681(a)(1)(A). Second, CIRCIA requires a covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity to report that payment to CISA. 6 U.S.C. 681b(a)(2)(A). Third, CIRCIA requires that, until a covered entity notifies CISA that the covered cyber incident in question has concluded and been fully mitigated and resolved, a covered entity must submit an update or supplement to a previously submitted report on a covered cyber incident if substantial new or different information becomes available. 6 U.S.C. 681b(a)(3). Finally, CIRCIA requires that a covered entity submit an update or supplement to a previously submitted report on a covered cyber incident if the covered entity makes a ransom payment after submitting a Covered Cyber Incident Report. 6 U.S.C. 681b(a)(3). CISA is proposing to incorporate these requirements in § 226.3 of the proposed regulation. Other parts of the proposed regulation discuss the report submission deadlines (§ 226.5; IV.D.iv), manner and form (§ 226.6; IV.D.i and ii), and information required (§§ 226.7 through 226.11; IV.D.iii) for all of these types of reports.

CISA is proposing to include the first reporting requirement, the requirement for a covered entity to report a covered cyber incident, in § 226.3(a). A covered entity would comply with this requirement by submitting, or having a third-party submit on the covered entity's behalf, a Covered Cyber Incident Report or a Joint Covered Cyber Incident and Ransom Payment Report pursuant to § 226.3(c). Cyber incidents do not occur in a single moment in time, but span from the initial moment of compromise until the cyber incident is fully mitigated and resolved. Because of this, CISA interprets the word "experiences" (in the statutory phrase "a covered entity that experiences a covered cyber incident") to include the full lifecycle of a cyber incident, such

that this reporting requirement applies to any entity that qualifies as a covered entity at any point during the occurrence of the covered cyber incident. For example, this means that if an entity discovers that it experienced a covered cyber incident two years ago that has continued to the present, and that entity is a covered entity at the time of discovery, the entity would be required to submit a Covered Cyber Incident Report under the proposed rule because the incident has not concluded and been fully mitigated and resolved. Conversely, if that same entity was not a covered entity at the time of discovery, but was one year ago (*i.e.*, during the period when the covered cyber incident was ongoing but not yet discovered), the entity would be required to submit a Covered Cyber Incident Report under the proposed rule because the entity experienced at least part of the covered cyber incident while it was a covered entity.

CISA is proposing to include the second reporting requirement, the requirement for a covered entity to report a ransom payment it has made, in § 226.3(b).³²⁸ CISA understands CIRCIA as requiring a covered entity to report a ransom payment regardless of whether the ransomware attack that led to the ransom payment is a covered cyber incident. 6 U.S.C. 681b(a)(2)(B). Additionally, CISA interprets 6 U.S.C. 681b(d)(3) to require a covered entity to report a ransom payment regardless of whether the covered entity itself makes the ransom payment or has a third-party make the ransom payment on the covered entity's behalf. Because this reporting requirement is tied to a single action that occurs at a specific moment in time—the making of a ransom payment—CISA interprets the word "makes" (in the statutory language "a covered entity that makes a ransom payment") to apply this reporting requirement to any entity that qualifies as a covered entity at the moment in time that it makes a ransom payment as the result of a ransomware attack.

Depending on the circumstances surrounding and timing of the ransom payment, including whether the ransomware attack is a covered cyber incident, the type of CIRCIA Report a covered entity (or third party on behalf

³²⁸ While the proposed rule includes reporting of ransom payments to CISA, as CIRCIA requires, CISA notes that "[t]he U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks." Department of the Treasury, Office of Foreign Asset Control, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021).

of a covered entity) might use to comply with proposed § 226.3(b) may vary. For example, if the ransom payment was made as the result of an incident that did not qualify as a covered cyber incident, the covered entity would submit a Ransom Payment Report under § 226.3(b). If the ransom payment was made as the result of a covered cyber incident that has not yet been reported, the covered entity may opt to submit a Joint Covered Cyber Incident and Ransom Payment Report under § 226.3(c) instead of a Covered Cyber Incident Report under § 226.3(a) and a separate Ransom Payment Report under § 226.3(b). Alternatively, if the ransom payment was made as the result of a covered cyber incident that the covered entity has previously reported to CISA, then the covered entity would use a Supplemental Report under § 226.3(d) to report the ransom payment to CISA.

Pursuant to 6 U.S.C. 681b(a)(5)(A), a covered entity that makes a ransom payment associated with a covered cyber incident prior to the expiration of the 72-hour reporting timeframe for reporting the covered cyber incident may submit a single report to satisfy both the covered cyber incident and ransom payment reporting requirements. CISA is proposing to include this option in § 226.3(c). Additional details on this type of joint report, which CISA is proposing to call a Joint Covered Cyber Incident and Ransom Payment Report, can be found in Section IV.A.iii.4 and IV.E.ii.1 of this document.

Lastly, CISA is proposing to include in § 226.3(d) the statutory reporting requirements that mandate a covered entity provide CISA with updates or supplements in certain circumstances. As discussed in Section IV.A.iii.5 of this document, CIRCIA refers to these types of reports as Supplemental Reports, which a covered entity is obligated to provide unless and until it has notified CISA that the underlying covered cyber incident has concluded and been fully mitigated and resolved. 6 U.S.C. 681b(a)(3). CISA's proposed interpretation for "concluded" and "fully mitigated and resolved" and the process for informing CISA of the belief that the covered cyber incident at issue has concluded and been fully mitigated and resolved are discussed in further detail in Sections IV.E.iv.3.c and IV.E.v.2 of this document, respectively. Notifying CISA that the covered entity believes the underlying covered cyber incident has concluded and been fully mitigated and resolved is optional.

The first scenario resulting in the requirement to submit a Supplemental Report is when substantial new or

different information becomes available to a covered entity. As with the covered cyber incident reporting requirement described above, CISA interprets this requirement as applying to an entity that is a covered entity during any point in the incident lifecycle, such that any entity that qualifies as a covered entity for the purposes of the covered cyber incident reporting requirement is also subject to the supplemental reporting requirement to the extent new or different information becomes available.

The second scenario resulting in the requirement to submit a Supplemental Report is when a covered entity makes a ransom payment related to a covered cyber incident for which the covered entity has already submitted a Covered Cyber Incident Report. As with the ransom payment reporting requirement described above, CISA interprets this requirement as applying to an entity that is a covered entity at the time a ransom payment is made, assuming they also were subject to the covered cyber incident reporting requirement described above.

These two scenarios that require the submission of a Supplemental Report are enumerated in §§ 226.3(d)(1)(i) and (ii), respectively.

ii. Reporting of Single Incidents Impacting Multiple Covered Entities

CISA anticipates that occasions will occur where a single cyber incident causes substantial cyber incident-level impacts to multiple covered entities. Who must report and the number of reports that must be submitted in those situations may vary depending on the relationship between the impacted entities.

In cases where a single cyber incident impacts multiple unaffiliated covered entities, each covered entity that experiences substantial cyber incident-level impacts must submit a Covered Cyber Incident Report to CISA. For example, if a compromise of a CSP causes substantial cyber incident level-impacts at multiple unaffiliated customers of the CSP, more than one of whom is a covered entity, then each of the impacted customers that are covered entities are responsible for submitting (or having a third party submit on their behalf) a Covered Cyber Incident Report. The covered entity customers could, however, authorize the CSP to submit Covered Cyber Incident Reports on their behalf under § 226.12(a) if the CSP has or is provided with sufficient information to complete the Covered Cyber Incident Reports. The CSP may also have to separately submit a Covered Cyber Incident Report if it is itself a covered entity and it experiences

threshold impacts that meet the definition of a substantial cyber incident.

Conversely, in cases where a single cyber incident causes substantial cyber incident-level impacts at multiple affiliated covered entities, the covered entities can meet their reporting obligations through either (a) the submission of a single Covered Cyber Incident Report that provides the required information on all of the impacted entities, or (b) multiple Covered Cyber Incident Reports, with one or more covered entities submitting their own reports. Examples of scenarios where multiple affiliated covered entities may experience impacts from a single substantial cyber incident include a substantial cyber incident that impacts a parent corporation and one or more of its subsidiaries; a cyber incident that impacts a number of SLTT Government Entities within the same jurisdiction (e.g., an incident that impacts a single county's general government network, the county's 911 system, and the county's school district network); or a cyber incident affecting a jointly operated venture that impacts downstream systems that are individually owned by members of the joint venture. In these and similar cases, the impacted covered entities may satisfy their reporting requirements under CIRCIA through the submission of a single Covered Cyber Incident Report so long as that report details the impacts experienced by each of the affected covered entities, any other required covered entity-specific details, and point(s) of contact who individually or collectively represent all of the covered entities on whose behalf the Covered Cyber Incident Report is being submitted.

Similarly, in cases where a cyber incident impacts a facility that has separate owners and operators, both of whom qualify as a covered entity, only a single Covered Cyber Incident Report is required. Thus, for example, if a cyber incident impacts a critical access hospital or a Community Water System that is owned by one entity and operated by another, the reporting obligations of both the owner and operator can be met by a single Covered Cyber Incident Report submitted by (or on behalf of) either the owner or the operator. However, both are separately obligated to ensure that at least one Covered Cyber Incident Report is submitted.

While the examples provided above focus on Covered Cyber Incident Reports, the principles being described apply equally to all types of CIRCIA Reports. Accordingly, if a ransom

payment is made on behalf of multiple affiliated entities, a single Ransom Payment Report can be submitted on their collective behalf. Similarly, affiliated entities may opt to submit a single Supplemental Report detailing substantial new or different information that impacts multiple affiliated covered entities. By contrast, if a supply chain compromise results in multiple covered entity customers of a single service provider experiencing a ransomware attack and each paying a ransom payment, each covered entity that makes a ransom payment is responsible for submitting a Ransom Payment Report.

D. Exceptions to Required Reporting on Covered Cyber Incidents and Ransom Payments

Section 681b(a)(5) of title 6, United States Code, contains three scenarios in which a covered entity is excepted from having to report a separate covered cyber incident or ransom payment. The first of these exceptions authorizes a covered entity to submit a single CIRCIA Report containing information on both a covered cyber incident and ransom payment when the covered entity makes a ransom payment related to a covered cyber incident within the 72-hour window for reporting the covered cyber incident. 6 U.S.C. 681b(a)(5)(A). The second exception allows a covered entity to forgo providing an otherwise required CIRCIA Report to CISA if it is legally required to report substantially similar information within a substantially similar timeframe to another Federal agency with whom CISA has an information sharing agreement and mechanism. 6 U.S.C. 681b(a)(5)(B). The third exception states that CIRCIA reporting requirements shall not apply to certain covered entities, or specific functions of those entities, that are owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the DNS. 6 U.S.C. 681b(a)(5)(C). CISA additionally is proposing a fourth exception that would exempt Federal agencies from having to submit a CIRCIA Report to CISA if the Federal agency is required to report the incident in question to CISA pursuant to FISMA, 44 U.S.C. 3551 *et seq.*

The first exception, which requires the submission of a Joint Covered Cyber Incident and Ransom Payment Report, is discussed in Section IV.E.ii of this document. The following subsections discuss the remaining three exceptions.

i. Substantially Similar Reporting Exception

Pursuant to 6 U.S.C. 681b(a)(5)(B), a covered entity that is required by law, regulation, or contract to report substantially similar information on a covered cyber incident or ransom payment to another Federal agency in a substantially similar timeframe as that required under CIRCIA does not have to submit a covered cyber incident Report or Ransom Payment Report to CISA on that covered cyber incident or ransom payment if CISA has an information sharing agreement and mechanism in place with that Federal agency. Under that same provision of CIRCIA, a covered entity is excepted from having to submit a Supplemental Report to CISA if the entity is required to provide to another Federal agency substantially similar information to that which the entity would otherwise be obligated to provide to CISA in a Supplemental Report, must do so in a substantially similar timeframe as that required under CIRCIA, and CISA has both an information sharing agreement and mechanism in place with the other Federal agency. This reporting exception (hereinafter the substantially similar reporting exception) will allow covered entities subject to more than one Federal cyber incident reporting requirement to avoid having to report duplicative information to both CISA and another Federal agency when certain conditions are met.

CISA interprets the statutory language to require five criteria for the application of the substantially similar reporting exception to apply: (1) the report must be required to contain substantially similar information to that required to be included in the applicable CIRCIA report; (2) the report must be required to be provided to the other Federal agency in a timeframe that allows CISA to receive the report in a substantially similar timeframe to that which the covered entity would otherwise have been obligated to provide the report to CISA pursuant to CIRCIA; (3) CISA and the Federal agency to which the covered entity submits the report must have an information sharing agreement in place that satisfies the requirements of 6 U.S.C. 681g(a) (hereinafter a CIRCIA Agreement); (4) CISA and the Federal agency to which the covered entity submits the report must have a mechanism in place by which the Federal agency can share the report with CISA within the required timeframe; and (5) the covered entity must have submitted the report to the other Federal

agency pursuant to a legal, regulatory, or contractual obligation.

CISA is proposing to only enter into a CIRCIA Agreement when CISA has determined that the Federal agency with whom CISA is entering into the agreement receives cyber incident reports from one or more CIRCIA covered entities pursuant to a legal, regulatory, or contractual obligation, and the reporting obligation requires the submission of substantially similar information in a substantially similar timeframe.³²⁹ When assessing whether another reporting obligation requires reporting of substantially similar information in a substantially similar timeframe to CIRCIA, CISA intends to coordinate with the Federal department or agency responsible for the non-CIRCIA reporting obligation which will inform CISA's decision making process.

If and when CISA has entered into a CIRCIA Agreement, CISA will announce and catalogue the existence of the CIRCIA Agreement on a public-facing website. In accordance with 6 U.S.C. 681g(a)(5)(B), to the extent practicable, CISA will publish the full CIRCIA Agreement. The listing of a CIRCIA Agreement by CISA demonstrates that CISA has determined that the applicable law, regulation, or contractual obligation requires a covered entity to report substantially similar information related to a covered cyber incident or ransom payment within a substantially similar timeframe and that the Federal agency has committed to providing the covered entity's report to CISA within the relevant deadlines under this Part. If a covered entity submits a report related to a covered cyber incident or ransom payment to another Federal agency with which CISA has an active and published CIRCIA Agreement, the covered entity's report qualifies for the exception under this section. If no CIRCIA Agreement is listed for a Federal agency, this exception does not apply, and reporting to that Federal agency will not exempt a covered entity from having to report directly to CISA in accordance with this part. A covered entity is responsible for confirming that a CIRCIA Agreement is applicable to both it and the specific CIRCIA reporting obligation that it is seeking to satisfy. CISA generally anticipates that each CIRCIA Agreement will describe or otherwise identify the

³²⁹ CISA may enter into other information sharing agreements with Federal agencies that do not meet the substantially similar reporting exception criteria; however, such agreements would not be considered CIRCIA Agreements and would not indicate the applicability of the substantially similar reporting exception to entities submitting reports to the Federal entity with which CISA entered into the agreement.

scope of entities and/or reporting obligations that are the subject of the CIRCIA Agreement.

If a law, regulation, or contract that serves as the basis for a CIRCIA Agreement is modified in any way, CISA may reassess if the respective law, regulation, or contract continues to meet the requirements necessary for that law, regulation, or contract to serve as the basis for application of the substantially similar reporting exception. CISA may terminate a CIRCIA Agreement at any time as long as doing so would not violate any aspect of the agreement itself. If CISA terminates a CIRCIA Agreement for any reason, CISA will provide notice of the termination on the public-facing website where the catalog of active CIRCIA Agreements is maintained.

1. Substantially Similar Information

To qualify for the substantially similar reporting exception, the information reported by a covered entity on a covered cyber incident or ransom payment to another Federal agency must be substantially similar to the information that the covered entity would be required (but for the exception) to report to CISA under this Part. CISA does not intend to define what constitutes substantially similar information in the final rule. Rather, CISA proposes to retain discretion in making this determination. In determining whether information is substantially similar, CISA will consider whether the information required by the fields in CISA's CIRCIA Report forms is functionally equivalent to the information required to be reported by the covered entity to another Federal agency. CISA views functionally equivalent as meaning that the information or data serves the same function or use, provides the same insights or conclusions, and enables the same analysis as the information or data requested in the relevant CIRCIA Report form fields.

CISA does not believe that the substantially similar information qualifier requires information to be reported in the same format to the other Federal agency. Other Federal agency reporting forms are unlikely to precisely mirror the CIRCIA Report. A covered entity could submit information in another Federal agency's reporting form that, while not directly aligning with a specify query in a CIRCIA Report form, nonetheless provides functionally equivalent data. CISA's determination that information is substantially similar will hinge on whether the data and information required to be submitted in a CIRCIA Report form are substantively

included in the report to the other Federal agency.

2. Substantially Similar Timeframe

To qualify for this exception, the covered entity must also be required to report this information to another Federal agency under law, regulation, or contractual provision in a substantially similar timeframe. In interpreting this requirement, CISA has to keep in mind the limitations related to sharing of reports pursuant to a CIRCIA Agreement, as set forth in 6 U.S.C. 681g(a)(5)(C). Specifically, that section requires that Federal agencies who share reports with CISA pursuant to a CIRCIA Agreement must do so "in such time as to meet the overall timeline for covered entity reporting of covered cyber incidents and ransom payments." 6 U.S.C. 681g(a)(5)(C).

When read together, CISA interprets these statutory requirements to render the substantially similar reporting exception available only if CISA receives the report on a covered cyber incident or ransom payment from the other Federal agency within the same timeframe in which the covered entity would have been required to submit the report to CISA under CIRCIA had the covered entity reported directly to CISA. Thus, for a law, regulation, or contractual provision to require reporting within a "substantially similar timeframe" of CIRCIA, it must require a covered entity to report a covered cyber incident within 72 hours from when the covered entity reasonably believes that the covered cyber incident has occurred and a ransom payment within 24 hours after the ransom payment has been disbursed, leaving the Federal agency time to share the report with CISA, unless a mechanism is in place that allows CISA to receive the report at the same time as the other Federal agency. For example, a law, regulation, or contractual provision that requires a covered entity to report a covered cyber incident to a Federal agency within 36 hours after discovery would have a substantially similar timeframe for the purpose of this exception. The Federal agency would have an additional 36 hours in which to share the report with CISA to meet the CIRCIA deadline for Covered Cyber Incident Reports.³³⁰ If a

³³⁰ Of note, CIRCIA separately provides that any Federal agency, including any independent establishment, that receives a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to CISA as soon as possible, but not later than 24 hours after receiving the report, unless a shorter period is required by a CIRCIA Agreement between CISA and the recipient Federal agency. 6 U.S.C. 681g. This requirement would apply to reports that are subject to the substantially similar reporting exception as well,

law, regulation, or contractual provision required a covered entity to report a covered cyber incident to a Federal agency within 72 hours of the covered entity reasonably believing a qualifying cyber incident occurred, the Federal agency would need to have a mechanism in place to share the report with CISA instantaneously upon receipt for it to be received by CISA in a substantially similar timeframe in compliance with the deadline for a Covered Cyber Incident Report under this part.

As discussed in Section IV.E.iv.1 of this document, a covered entity must report a covered cyber incident within 72 hours after it "reasonably believes" a covered cyber incident occurred. CISA recognizes that not all incident reporting requirements in law, contract, or regulation have the same trigger for "starting the clock" on when an incident becomes reportable, and that different triggers could result in dramatically different reporting timeframes even if the numerical timeframes were substantially similar. For instance, a regulation that requires reporting within 24 hours of confirmation of a reportable incident could in fact have a reportable timeframe that effectively is substantially longer than CIRCIA's 72-hour reporting timeframe as "confirmation" of a reportable incident could occur days or weeks after a "reasonable belief" that a reportable incident occurred is established. In determining whether to enter into a CIRCIA Agreement with another Federal agency, CISA will take into account when the reporting timeframe is triggered under the governing law, regulation, or contract.

3. Supplemental Reporting

Supplemental Reports may also qualify for the substantially similar reporting exception, provided that the supplemental report provided to the other Federal agency meets the relevant requirements. As with a Covered Cyber Incident Report or Ransom Payment Report, the exception is only available if the covered entity is required to submit substantially similar information in a substantially similar timeframe to another Federal agency under law, regulation, or contract and CISA and the other agency have a CIRCIA Agreement and information sharing mechanism in place to meet the CIRCIA Report deadlines. CIRCIA requires

and would therefore be relevant in determining whether a reporting timeframe is substantially similar while allowing for sufficient time for CISA to receive the report from the recipient Federal agency.

Supplemental Reports be submitted “promptly,” which CISA interprets as within 24 hours of the triggering event. See 6 U.S.C. 681b(a)(3) and Section IV.E.iv.3.a of this document. A covered entity remains responsible for submitting Supplemental Reports to CISA as required under this Part unless the covered entity submits any substantial new or different information to another Federal agency and CISA has published a CIRCIA Agreement with that Federal agency that specifically covers Supplemental Reports.

4. Communications With CISA

The exception under this section does not prevent CISA from contacting the covered entity about the information it provided to the other Federal agency. 6 U.S.C. 681b(a)(5)(B)(iii). Moreover, nothing in this section prohibits a covered entity from also submitting a CIRCIA Report to CISA even if the CIRCIA Report is qualified for an exception. 6 U.S.C. 681b(a)(5)(B)(iii).

5. Request for Comments

CISA seeks comments on its proposed approach to implementing the substantially similar reporting exception, to include:

38. CISA’s proposed interpretations of what constitutes substantially similar information and a substantially similar timeframe.

39. The application of the substantially similar reporting exception to Supplemental Reports.

40. The manner in which CISA proposes informing the public of the availability of this exception.

41. Any other aspects of the substantially similar reporting exception.

ii. Domain Name System (DNS) Exception

Pursuant to 6 U.S.C. 681b(a)(5)(C), the CIRCIA reporting requirements “shall not apply to a covered entity or the functions of a covered entity that the Director determines constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority.” Based on this language, CISA is proposing to create an exception from CIRCIA reporting requirements for ICANN, the American Registry for Internet Numbers (ARIN), and affiliates of those entities. CISA additionally proposes to create a limited exception from CIRCIA reporting requirements for the DNS Root

Server Operator (RSO) function of a covered entity.

To qualify for the reporting exception provided in 6 U.S.C. 681b(a)(5)(C), a covered entity must have been determined by the Director to meet two criteria. First, the Director must have determined that the covered entity constitutes critical infrastructure. Second, the Director must have determined that the covered entity, or a specific function of that entity, is owned, operated, or governed by a multi-stakeholder organization that develops, implements, and enforces policies concerning the DNS. As very few entities meet the second criterion, it is more efficient to begin CISA’s analysis on this topic by considering the second criterion first.

To determine what covered entities might meet the second criterion, CISA assessed the DNS ecosystem to identify multi-stakeholder organizations that develop, implement, and enforce policies concerning the DNS and to identify entities that are wholly owned, operated, or governed by such multi-stakeholder organizations. Based on this assessment, CISA believes that two specific entities meet this criterion, and a third category of entities meet the criterion as well.

The first entity that CISA has assessed is a multi-stakeholder organization that develops, implements, and enforces DNS policies is ICANN. ICANN is a not-for-profit, multi-stakeholder organization that leads the development of bottom-up, consensus policies and guidelines that help advance the stable and secure operation of the internet’s unique identifier systems and help define how the DNS functions.³³¹

The second entity that CISA has assessed as meeting this criterion is Public Technical Identifiers (PTI). PTI is a 501(c)(3) non-profit whose specific purpose is to operate exclusively to carry out the purposes of ICANN, which is a multi-stakeholder organization.³³² PTI is an affiliate of ICANN that is wholly controlled by ICANN, akin to complete ownership, thus meeting the “owned, operated, or governed by” a multi-stakeholder organization clause contained within CIRCIA’s statutory reporting exception.

The third group of covered entities that are multi-stakeholder organizations

with responsibilities related to the development, implementation, and enforcement of DNS policies are Regional Internet Registries (RIRs). RIRs are multi-stakeholder organizations responsible for managing, distributing, and registering internet number resources (IPv4 and IPv6 address space and Autonomous System (AS) Numbers) within their respective regions.³³³ Currently, there are five RIRs in the world: (1) the African Network Information Centre (AFRINIC), which services Africa and the Indian Ocean; (2) the Asia-Pacific Network Information Centre (APNIC), which services Asia and the Pacific; (3) ARIN, which services the United States, Canada, and many Caribbean and North Atlantic Islands; (4) the Latin American and Caribbean Internet Addresses Registry (LACNIC), which services Latin America and the Caribbean; and (5) the Réseaux IP Européens Network Coordination Centre (RIPE NCC), which services Europe, the Middle East, and parts of Central Asia.³³⁴ Since ARIN is the only RIR with a legal presence in the United States, CISA has assessed that ARIN is the only relevant RIR for purposes of CIRCIA.

Finally, CISA assessed whether the CIRCIA reporting exception should apply to any specific function of a covered entity that is owned, operated, or governed by a multi-stakeholder organization that develops, implements, and enforces policies concerning the DNS. Given the RSO’s role in operationalizing a specific, critical IANA function of overseeing operation of the internet root server system, CISA has assessed that the DNS RSO function also meets this criterion.

The Internet Assigned Numbers Authority functions (IANA functions) are administered by PTI, which is owned by ICANN, a multi-stakeholder organization responsible for development, implementation, and enforcement of policies concerning the DNS.³³⁵ One of the key IANA functions is the management of the DNS root zone.³³⁶ The “root zone” is the uppermost part of the DNS hierarchy.³³⁷ The root zone management function uses the Root Server System (RSS) for publication of the root zone. The RSS is

³³³ See NRO, *Regional Internet Registries*, <https://www.nro.net/about/rirs/> (last visited July 24, 2023).

³³⁴ *Id.*

³³⁵ See U.S.C./ICANN Transition Agreement, ICANN, available at <https://www.icann.org/resources/unthemed-pages/usc-icann-transition-2012-02-25-en>.

³³⁶ See IANA, *Root Zone Management*, <https://www.iana.org/domains/root> (last visited Nov. 14, 2023).

³³⁷ See IANA, *Domain Name Services*, <https://www.iana.org/domains> (last visited Nov. 15, 2023).

³³¹ See ICANN, *Policy Mission*, <https://www.icann.org/resources/pages/mission-2012-08-27-en> (last visited July 24, 2023); see also ICANN, *ICANN For Beginners*, <https://www.icann.org/get-started> (last visited July 24, 2023).

³³² See PTI Articles of Incorporation Sections II and III. The PTI Articles of Incorporation are available at <https://pti.icann.org/articles-of-incorporation> (last visited Nov. 13, 2023). See also later discussion of the IANA functions.

administered collectively by the RSOs, which serve as the authorities for each of the A, B, C, D, E, F, G, H, I, J, K, L, and M root servers. The root servers operated by the RSOs act exclusively as a mechanism by which the content of the root zone database is made publicly available. This activity is largely viewed by the DNS ecosystem as an operationalization of the historic IANA root zone management function on behalf of ICANN.³³⁸ ICANN manages matters related to the operation, administration, security, and integrity of the internet root server system through the Root Server System Advisory Committee (RSSAC), which is an advisory committee created by ICANN to advise the ICANN community and board.³³⁹ As part of RSSAC's advice, it has also defined a set of service expectations that RSOs have agreed to satisfy.³⁴⁰

CISA has assessed that the RSO function is an operationalization of ICANN's responsibility to operate the internet root server system and thus qualifies as a "function[]" of a covered entity . . . owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority." Accordingly, CISA has assessed that the RSO function of a covered entity that has been recognized by ICANN as responsible for operating one of the 13 root identities and agrees to follow the service expectations established by the RSSAC and ICANN may qualify for the DNS Exception, if the second criterion for the DNS Exception is met, (*i.e.*,

whether the function also constitutes critical infrastructure).³⁴¹

Note, to the extent the proposed DNS Exception may apply to a covered entity that is an RSO, it would only apply to the RSO function of the entity. Other functions performed by an RSO that are not the RSO function would not qualify for the proposed DNS Exception under CIRCIA. Accordingly, should an RSO that is also a covered entity experience a covered cyber incident or make a ransom payment as the result of a ransomware attack that impacts the entity's activities or business streams that are separate from, or in addition to, its RSO function, the covered entity would be required to report that covered cyber incident or ransom payment under this proposed regulation.

For a covered entity to be eligible for an exception from CIRCIA reporting requirements under the proposed DNS Exception, it must also meet the first criterion included in the statutory language—*i.e.*, be determined by the Director to constitute critical infrastructure. The USA Patriot Act (Pub. L. 107–56) and, by reference, both the Homeland Security Act of 2002, as amended, and PPD–21 define "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."³⁴² Given their roles in ensuring the functioning of the DNS around the world, and the debilitating impacts a significant failure of the DNS would have on national security, economic security, or public health, and safety, the Director has determined that ICANN, ARIN, and their affiliates³⁴³ (such as PTI) meet the

definition of critical infrastructure for purposes of applying this statutory exception. The Director also has determined that, given the criticality of the DNS root zone to the operation of the internet, the RSO function performed by a covered entity qualifies as critical infrastructure as well.

Based on the aforementioned analysis, ICANN, ARIN, any affiliates of ICANN or ARIN (such as PTI), and the RSO function of covered entities meet both criteria contained in the statute for the DNS Exception. Accordingly, CISA proposes in § 226.4(b) that ICANN, ARIN, and their affiliates do not need to report to CISA covered cyber incidents that they experience or ransom payments they make as the result of a ransomware attack. CISA further proposes to exempt a covered entity from CIRCIA reporting requirements for covered cyber incidents and ransom payments made as a result of a ransomware attack that solely relate to the entity's RSO function.

Given the complexities of the DNS, as well as the long-standing U.S. Government policy goal of support of the multi-stakeholder approach to internet governance that may impact other entities in this space, CISA recognizes the importance of public feedback on the scoping of this reporting exception consistent with the legal requirements in 6 U.S.C. 681b(a)(5)(C) and the purposes for which CIRCIA has been established. In particular, CISA welcomes comments on all aspects of this topic. Among other things, CISA welcomes comments on the possible application of the DNS exception to domain name registries and registrars, and of all associated questions of law and policy. CISA will give extreme careful consideration to alternative views, including the possible application of the DNS exception to domain name registries and registrars. Consistent with Executive Order 13563, CISA is strongly committed to public participation, to maintaining openness, and to serious assessment of alternative approaches that might better balance the relevant interests. CISA invites submission of views, information, data, and comments on the following policy and legal questions that are unique to the DNS community:

technical individual might actually consider them to be part of ICANN or ARIN.

³³⁸ See IANA, *Root Zone Management*, <https://www.iana.org/domains/root> (last visited Nov. 14, 2023); see also ICANN, *Brief Overview of the Root Server System*, at 4 (May 6, 2020), available at <https://www.icann.org/en/system/files/files/octo-010-06may20-en.pdf> ("The 13 root services respond to the queries they receive either with information found in the root zone as it is managed by the IANA Functions operated by ICANN. . .").

³³⁹ You can find more information about the RSSAC at <https://www.icann.org/groups/rssac#:~:text=Root%20Server%20System%20Advisory%20Committee%20%20,31%20December%202024%20%208%20more%20rows%20> (last visited Nov. 28, 2023).

³⁴⁰ RSSAC001, *Service Expectations of Root Servers*, Version 1 (Dec. 4, 2015) available at <https://www.icann.org/en/system/files/files/rssac-001-root-service-expectations-04dec15-en.pdf>.

³⁴¹ There currently are 12 RSOs that perform the IANA root zone management function: Verisign, Inc.; the University of Southern California, Information Sciences Institute; Cogent Communications; the University of Maryland; NASA; Internet Systems Consortium, Inc.; the U.S. Department of Defense (NIC); the U.S. Army Research Lab; Netnod; RIPE NCC; ICANN; and WIDE Project. Verisign, Inc. manages two of the root identities. See IANA, *Root Servers*, <https://www.iana.org/domains/root/servers> (last visited Nov. 14, 2023).

³⁴² 42 U.S.C. 5195c(e).

³⁴³ "Affiliates" in this context is meant to reflect entities that have been recognized by ICANN or IANA/ARIN as an affiliate and are so significantly controlled by ICANN or ARIN that the average non-

42. The covered entities which CISA proposes this exception apply to, including whether any additional covered entities involved in DNS operations, such as domain name registries and registrars, should be considered by CISA for this reporting exception. If so, how do those covered entities, or specific functions thereof, meet the statutory requirements, including specifically how the entity or its functions may “constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the internet Corporation for Assigned Names and Numbers or the internet Assigned Numbers Authority”?

43. Information, facts, or other views that describe or explain the relationship between ICANN and domain name registries and registrars, as well as specific cyber incident and ransom payment information that must be reported to ICANN by entities accredited by ICANN.

44. What types of covered cyber incidents could be unique to, or have a unique impact on, the covered entities that would be exempt from reporting under CIRCIA based on the scoping of the proposed DNS Exception?

45. What are the potential consequences of covered cyber incidents that would not be reported to CISA based on the proposed DNS Exception (*e.g.*, impacts to the functionality of the internet or to services offered to critical infrastructure)?

46. What are the specific technical functions that DNS entities perform or provide in order to support the DNS versus related, but separate commercial offerings? How would this apply to different DNS entities such as root server operators, domain name registries, and domain name registrars?

47. What cyber incident reporting requirements, either in the United States or internationally, are DNS entities currently subject to? To what government agency or other entity must those entities report cyber incidents? Please describe the specific cyber incident reporting requirement (*e.g.*, timing and trigger requirements; details that must be reported; mechanism for reporting; supplemental reporting requirements).

48. How should the U.S. government’s support for the multi-stakeholder system of internet governance inform the DNS Exception?

49. Any other aspects of CISA’s proposed approach to the DNS Exception.

iii. Exception for Federal Agencies Subject to Federal Information Security Modernization Act Reporting Requirements

CISA also is proposing to exempt Federal agencies required by FISMA (44 U.S.C. 3551 *et seq.*) to report incidents to CISA from reporting those incidents as covered cyber incidents under CIRCIA. FISMA requires Federal agencies (as defined in 44 U.S.C. 3502), except for systems identified in 44 U.S.C. 3553(d) and (e), to notify CISA regarding information security incidents involving their information and information systems, whether managed by a Federal agency, contractor, or other source.

While the definition for substantial cyber incident under the CIRCIA regulation will not be finalized until CISA completes the rulemaking process, CISA anticipates that all incidents that ultimately will constitute substantial cyber incidents would also be considered reportable incidents under FISMA if experienced by a Federal agency. Similarly, CISA anticipates that the content that Federal agencies must submit in reports required under FISMA will be substantially similar to the information required in CIRCIA Covered Cyber Incident Reports. Finally, FISMA requires reporting by Federal agencies to CISA in a shorter timeframe—one hour from the time of identification of the incident—than is required under CIRCIA. In light of this, CISA expects to already be receiving substantially similar information from FISMA-covered Federal agencies on all substantial cyber incidents within a shorter timeframe than required by CIRCIA. For these reasons, CISA is proposing to exempt FISMA-covered Federal agencies that are required by FISMA to report incidents to CISA from having to submit a CIRCIA Report for those incidents that constitute covered cyber incidents. Per the terms of this exception, as proposed in § 226.4(c), this exception only applies to Federal agencies, and does not exempt government contractors or subcontractors from any otherwise-required CIRCIA reporting.

Other cyber incident reporting regulations may exist for which entities may be required to provide other Federal departments or agencies with similar information about substantial cyber incidents in a similar or shorter timeframe than that which is required under CIRCIA. CISA is not offering a similar exclusion to entities based on those reporting requirements. CISA is proposing to exclude Federal agencies subject to cyber incident reporting

under FISMA, but not entities subject to other Federal cyber incident reporting requirements, because CISA believes FISMA differs from those other regulations in two important ways. First, because CISA is the Federal entity responsible for implementing FISMA, CISA has control (within the boundaries of any limitations established by Congress in the FISMA authorizing legislation) over the types of incidents that must be reported, the content that must be included in those reports, and the timeframe for submission of those reports. CISA does not have similar control over those aspects of reporting required by other regulatory programs. As a result, CISA has no ability to ensure that those regulatory programs continue to require incident reports with substantially similar information for substantial cyber incidents in a substantially similar timeframe. Second, because the statutory requirements for using the substantially similar reporting exception—*e.g.*, the information is required to be reported “to another Federal agency”—explicitly address situations involving CISA and a different Federal regulator, CISA is unable to leverage the substantially similar reporting exception to avoid duplicative reporting for requirements such as FISMA where CISA is the entity responsible for overseeing the reporting requirement. To avoid duplicative reporting requirements in situations where CISA is the entity receiving reports under two requirements, CISA needs to specifically exempt entities subject to those requirements from CIRCIA reporting requirements or otherwise make it clear in either the CIRCIA regulations or the other reporting requirements that submission of a CIRCIA Report satisfies both reporting requirements. For reporting requirements that require reporting to a different Federal agency, the substantially similar reporting exception is the proper approach for seeking to avoid duplicative reporting requirements.

To the extent other regulations exist that require a covered entity to submit cyber incident reports containing substantially similar information to that required in CIRCIA Reports to another Federal entity in a substantially similar timeframe to that required under CIRCIA, CISA intends to work with that Federal entity to explore the possibility of enabling the covered entity’s submission to the other Federal entity to satisfy the covered entity’s CIRCIA incident reporting requirements. This would be done consistent with the substantially similar reporting exception

authorized in 6 U.S.C. 681b(a)(5)(B) of CIRCIA. Additional information on the substantially similar reporting exception, and the process CISA will undertake to implement it, can be found in Section IV.D.i of this document.

CISA seeks comments on its proposed exception for Federal agencies subject to FISMA reporting requirements, to include:

50. The establishment of the FISMA reporting exception.

51. Any aspects of CISA's proposed approach to implementing the FISMA reporting exception.

E. Manner, Form, and Content of Reports

i. Manner of Reporting

1. Overview

Pursuant to 6 U.S.C. 681b(a)(6) of CIRCIA, covered entities must make CIRCIA Reports in the manner and form prescribed in the final rule. CIRCIA requires CISA to include procedures for submitting these reports in the final rule, including the manner and form thereof. 6 U.S.C. 681b(c)(8)(A). CIRCIA gives CISA broad discretion in determining the manner and form for submission of CIRCIA Reports, although 6 U.S.C. 681b(c)(8)(A) requires CISA to "include, at a minimum, a concise, user-friendly web-based form" as one manner for submission of required reports.

CISA has direct experience using a web-based form to receive cyber incident reports, as that is the primary manner in which CISA has been receiving cyber incident reports from external stakeholders for a number of years. CISA also has experience receiving voluntarily submitted cyber incident reports from stakeholders telephonically and via email.

A variety of means for submitting cyber incident reports are currently in effect across the numerous Federal departments and agencies that require entities to report cyber incidents to them. A number of Federal departments and agencies use a web-based form or similar online submission system as the sole mechanism or one option for submitting required cyber incident reports. These include, among others,

DOD,³⁴⁴ DOE,³⁴⁵ TSA,³⁴⁶ SEC,³⁴⁷ and the NRC.³⁴⁸ Other commonly allowed methods for the submission of cyber incident reports include telephone, email, and automated (*i.e.*, machine-to-machine) reporting.³⁴⁹ At least one

³⁴⁴ See DOD—Defense Industrial Base Cyber Security Activities, 32 CFR 236.4(b)(2) (reports must be made electronically through <https://dibnet.dod.mil>). DOD does offer reporting telephonically if the dibnet is unavailable. See Defense Industrial Base Cybersecurity Portal Frequently Asked Questions, available at <https://dibnet.dod.mil/portal/intranet/#faq-4>.

³⁴⁵ DOE has established mandatory reporting requirements for electric emergency incidents and disturbances, to include those caused by cyber incidents. Entities within the electric power industry that have reportable incidents must use Form DOE-417 to report those incidents. DOE prefers that the form be submitted online through the DOE-417 Online System at <https://www.oe.netl.doe.gov/OE417/>, although DOE will also accept submissions via fax, telephone, or email. See DOE-417 Electric Emergency Incident and Disturbance Report (OMB No.: 1901-0288) at 1, available at <https://www.oe.netl.doe.gov/oe417.aspx>.

³⁴⁶ See, *e.g.*, *Security Directive 1580-21-01—Enhancing Rail Cybersecurity*, Section B.3 ("Reports required by this section must be made to CISA Central using CISA's Reporting System form at: <https://us-cert.cisa.gov/forms/report> or by calling (888) 282-0870."); *Security Directive 1582-21-01—Enhancing Public Transportation and Passenger Railroad Cybersecurity*, Section B.3 ("Reports required by this section must be made to CISA Central using CISA's Reporting System form at: <https://us-cert.cisa.gov/forms/report> or by calling (888) 282-0870."); *Security Directive Pipeline-2021-01—Enhancing Pipeline Cybersecurity*, Section C ("Reports must be made to CISA Central using CISA's Reporting System form at: <https://us-cert.cisa.gov/forms/report> or by calling (888) 282-0870."). Copies of these security directives are available at <https://www.tsa.gov/sd-and-ea>.

³⁴⁷ Regulation SCI Entities are required to use the Form SCI to notify the SEC of reportable incidents. A pdf version of Form SCI can be found at <https://www.sec.gov/files/form-sci.pdf> (last visited Nov. 28, 2023). Form SCI can be filed in an electronic format through the Electronic Form Filing System, a secure website operated by the SEC that can be accessed at <https://tts.sec.gov/effs/do/Index>.

³⁴⁸ The NRC's Cyber Security Event Notifications regulations require covered licensees to provide the NRC with initial notifications of cybersecurity events telephonically to the NRC Headquarters Operations Center via the Emergency Notification System. 10 CFR 73.77(c). For certain types of cyber security events, licensees must provide the NRC with written security follow-up reports using NRC Form 366. 10 CFR 73.77(d)(3). A copy of the web-based version of NRC Form 366 can be found at <https://www.nrc.gov/docs/ML1308/ML13083A106.pdf> (last visited Nov. 28, 2023).

³⁴⁹ See, *e.g.*, Federal Reserve Board, *Computer-Security Incident Notification Requirements*, 12 CFR 225.302 ("A banking organization must notify the appropriate Board-designated point of contact about a notification incident through email, telephone, or other similar methods that the Board may prescribe."); Office of the Comptroller of the Currency, *Computer-Security Incident Notification Requirements*, 12 CFR 53.3 ("A banking organization must notify the appropriate OCC supervisory office, or OCC-designated point of contact, about a notification incident through email, telephone, or other similar methods that the OCC may prescribe."); Federal Deposit Insurance Corporation, *Computer-Security Incident Notification Requirements*, 12 CFR 304.23 ("A

regulator does not articulate specific manners in which regulated entities must submit reports to it, leaving the manner up to the discretion of the reporting party.³⁵⁰

A majority of comments on this topic provided by stakeholders in response to the CIRCIA RFI and at CIRCIA listening sessions indicated support for the use of a web-based portal as a means for submission of reports to CISA. Some commenters recommended offering a web-based portal as either the only means or the preferred means of submission, while others suggested offering the web-based portal as simply one means of submission. One reason often provided by commenters advocating for the web-based portal to be one of multiple mechanisms for reporting was to ensure the existence of an alternative method of reporting should a covered cyber incident have rendered it difficult for the covered entity to submit a report via a web-based portal. Commenters expressing this rationale often suggested telephonic reporting as the recommended alternative option. A small number of commenters recommended that CISA offer the ability for covered entities to use automated (*i.e.*, machine-to-machine) reporting, email, or submit through other Federal departments or agencies' field office locations. See Section III.F.vi in this document for a summary of stakeholder comments on the manner and form of submission of CIRCIA Reports.

2. Proposed Approach

Section 226.6 of the proposed rule contains CISA's proposal for the manner of submission of CIRCIA Reports. CISA is proposing that a covered entity must

banking organization must notify the appropriate FDIC supervisory office, or an FDIC-designated point of contact, about a notification incident through email, telephone, or other similar methods that the FDIC may prescribe."); NCUA, *Cyber Incident Notification Requirements for Federally Insured Credit Unions Proposed Rule*, 87 FR 45029 (proposed rule would require "[e]ach federally insured credit union must notify the appropriate NCUA-designated point of contact of the occurrence of a reportable cyber incident via email, telephone, or other similar methods that the NCUA may prescribe."); see also FCC-NORS, 47 CFR part 4 (regulated entities can submit reports automatically through an approved NORS Application Programming Interface).

³⁵⁰ See, *e.g.*, Commodity Futures Trading Commission Designated Contract Markets System Safeguards regulations, 17 CFR 38.1051(e)(2) (requires designated contract markets to promptly notify CFTC staff of certain cybersecurity incidents, but does specify how notifications must be provided), 39.18(g) (requires derivatives clearing organizations to promptly notify CFTC staff of certain security incidents). While the CFTC's regulations do not specify how notifications must be provided, the CFTC has a portal for such notifications that is available to registrants.

submit CIRCIA Reports through the web-based CIRCIA Incident Reporting Form available on CISA's website or in any other manner approved by the Director.

As noted earlier, CIRCIA requires CISA to offer a web-based form as one manner of submission of CIRCIA Reports. See 6 U.S.C. 681b(c)(8)(A). Not only does CISA intend to offer a web-based form as a manner of submission of CIRCIA Reports, for several reasons CISA agrees with those commenters who suggested that an electronic, web-based form is the preferred manner for submission of CIRCIA Reports. First, a web-based form is a cost-effective way to gather information from large numbers of submitters both simultaneously and over time. If designed properly, it allows for significant standardization of data (in both form and content) and tailoring of circumstance-specific questions using dynamic prompts and responses incorporating conditional logic filters and conditional or branching questions. A web-based form can also reduce the likelihood of human error during the data submission process in various ways. For example, submission methods such as via telephone call require at least two individuals to facilitate the submission (*i.e.*, one person from the covered entity to provide CISA with information on the incident and another person from CISA to transcribe the information into CISA's information management system) and create the possibility of human error if one individual mishears, misspeaks, erroneously transcribes, or otherwise unintentionally enters incorrect data into the system. This is especially problematic for some of the data that CISA expects covered entities may often need to report, such as malware hashes or IP addresses, which typically are long strings of numbers and/or letters. A web-based form only requires the involvement of a single individual (*i.e.*, the person entering the information into the form on behalf of the covered entity) and allows for that individual to review information after entry but prior to submission, greatly reducing the potential for such errors.

Similarly, by using drop-down menus, radio buttons, or other limited response options where feasible and appropriate, a web-based form reduces the likelihood of human error resulting from the submitter not understanding the types of responses a question is seeking or CISA not understanding a narrative answer provided by a submitter. Third, a web-based form both allows for greater standardization of responses and does so in a machine-

readable format, and, in doing so, it facilitates a number of activities that are much more challenging when data is submitted in other manners. These activities include automated triage of reports; rapid, large-scale trend analysis; timely information sharing; and long-term storage, many of which CISA is required by CIRCIA to perform. Finally, a web-based form enables the submission of digital artifacts (*e.g.*, malware samples), which cannot be transmitted verbally.

Conversely, web-based forms present only a small number of potential drawbacks, each of which CISA believes are easily addressed. First, the government will incur costs to develop, maintain, and implement a web-based form. Depending on the options selected, existing resources, and other factors, the governmental costs associated with developing, maintaining, and implementing a web-based form may be greater or less than other potential methods of submission. In this case, however, the issue is effectively moot because, as noted earlier, CIRCIA requires that CISA offer a web-based form as a manner of submission. Consequently, CISA will have to incur the costs associated with a web-based form regardless of whether it is the sole, primary, or one of many options.

Second, a cyber incident at a covered entity could make it impossible or insecure for a covered entity to use its own information system(s) to report via a web-based form. CISA believes that this is a relatively minor concern, however, as organizations and individuals today typically have a variety of ways to access the internet. Additionally, CISA intends to make the web-based form available via a web browser so that incident reports can be submitted from any internet-connected device. This should allow covered entities various ways to access the form even if the entity's IT system is rendered inoperable by a cyber incident. Furthermore, CIRCIA permits a third party to submit CIRCIA Reports on a covered entity's behalf, such that even if the covered entity itself cannot report via a web-based form using its own information system(s) or any other internet connected device, any number of third parties should be able to submit the CIRCIA Report on the covered entity's behalf.

Third, there is the potential that an incident at CISA could render the web-form unavailable for use by covered entities for a period of time. CISA has extensive experience building systems that operate with high availability and intends to build in redundancy to

ensure the 24/7 availability of the reporting system. CISA also intends to maintain a capability to support reporting via telephone as a back-up option so that, in the unlikely event of an extended interruption of the availability of the web-based form, any impacted covered entities will have an alternative mechanism available to submit CIRCIA Reports in a timely manner. This or any other approved alternative mechanism also may be used in lieu of the web-based reporting system should a covered entity wish to submit a CIRCIA Report during any short-term unavailability of the system, such as if CISA must temporarily restrict access to the web-based form for routine maintenance.

On balance, CISA believes that the web-based form is the most useful and cost-effective manner for the submission and receipt of CIRCIA Reports and is proposing that as the sole explicitly identified option for submission of CIRCIA Reports.³⁵¹ CISA is also proposing to include in the rule the statement that covered entities may also submit CIRCIA Reports in any other manner and form of reporting approved by the Director. This provision would allow CISA to operate a telephonic reporting capability as a backup system and maintain flexibility to offer alternative manners of submission in the future on a short- or long-term basis. CISA believes that this flexibility is important for several reasons.

First, as mentioned in the previous paragraph, in the unlikely event of an extended interruption of the availability of the web-based form or other situation that renders it impossible for an entity to submit via the web-based form, this phrase would allow CISA the flexibility to establish other means to accept CIRCIA Reports in a rapid fashion. Second, as discussed further below, CISA believes that automated (*i.e.*, machine-to-machine) reporting has the potential to be a cost-effective method for some covered entities to submit CIRCIA Reports in the future. The "any other manner and form of reporting approved by the Director" clause will allow CISA the agility to more rapidly authorize entities to submit CIRCIA Reports via machine-to-machine reporting should CISA determine that is a viable, cost-effective approach in the future without having to undertake additional rulemaking. Similarly, this

³⁵¹ For similar reasons, CISA is considering encouraging entities that submit voluntary reports to CISA to do so through the CIRCIA web-based form; however, as noted in Section III.A, CISA is not proposing to address entirely voluntary reporting, including how such reports may be submitted, in this rulemaking.

provision will allow CISA the flexibility to consider and adopt new submission mechanisms that may become feasible as technology advances. CISA will publicize any additional manners of submission on its website and through notifications to stakeholders should the CISA Director approve any.

3. Additional Reporting Methods Options Considered

In deciding upon this proposed approach, CISA considered numerous options in addition to a web-based form. The additional options CISA considered are detailed in the following subsections. Each option has drawbacks that led CISA to determine not to offer them as a manner of submission at this time with the potential exception of a backup capability should the web-based form become unavailable for a period of time.

a. Telephone

One alternative manner CISA considered was telephonic submission of reports. Under this approach, a covered entity would be able to call CISA and verbally report the incident to CISA via telephone. To ensure that all of the necessary information is submitted and that the information is stored and made available to CISA in a manner consistent with the web-based form manner of submission, a CISA representative would ask the caller all of the pertinent questions in the web-based form and simultaneously fill out the web-based form on the caller's behalf.

The primary benefits of this approach include the ubiquity of and familiarity individuals have with telephones, their ease of use, the ability for a covered entity and a CISA representative to directly engage during the reporting process, the ability for CISA to ensure all necessary information is being submitted (including by asking real-time follow up questions), and the ability for CISA to ultimately capture information in a manner compatible with the statutorily required web-based form submissions. A few significant downsides with this approach exist, however. The first is the potentially significant additional cost to the government of manning a 24/7 telephone operation at a scale large enough to handle the receipt of all CIRCIA Reports. The second drawback is the added layer of potential transcription error introduced by requiring an individual other than the covered entity representative to physically enter the information into the web-based form. Beyond the potential for transcription error, it would likely take more time for a CISA telephone

operator to solicit, transcribe, and validate the information with the covered entity than to have a covered entity enter the same information directly into a web-based form.

In light of these drawbacks, CISA is not proposing to include telephonic reporting as a primary option. CISA does, however, intend to maintain telephonic reporting capabilities as a back-up option in case a covered entity is unable to submit a CIRCIA Report using the web-based form for some legitimate reason, such as an outage affecting the availability of the web-based form.

b. Email

CISA also considered the submission of CIRCIA Reports via email. Email could be used in two primary ways for the submission of reports. First, CISA could allow covered entities to use email to submit a standardized form (e.g., a fillable PDF form or a paper form that an entity could scan and attach to an email). Second, CISA could allow covered entities to submit required information via text contained in the body of the email itself without requiring any specific format or template be used.

Offering either manner of email submissions would provide a number of benefits. For instance, given the ubiquity of email in today's society and its availability on mobile devices, employees of covered entities are likely to have both familiarity with and access to email even if a cyber incident has rendered a covered entity's information systems inoperable. Similarly, email is a standard part of CISA operations, so CISA would be able to easily establish a mechanism to receive email submissions without having to expend significant upfront costs. Email generally also comes with automated tracking (via sent email folders), which can help the covered entity provide proof that a report has been submitted and the time and date of the submission.

There are, however, several major drawbacks associated with email submissions. First, as opposed to a web-based form where CISA could require certain questions be answered for the form to be submitted, or a telephone submission where a CISA employee could directly interact with the submitter to ensure all necessary information is provided, email does not provide a means for CISA to ensure that all required information is submitted before the report is made. Consequently, CISA envisions email submissions would result in a potentially significant number of cases in which CISA would need to follow up with the covered

entity to obtain required information. Limiting the use of email as a mechanism for the submission only of a fillable reporting form might somewhat reduce the need for follow-up when compared to allowing unbound email submissions; however, CISA believes this likely still would occur frequently.

Second, regardless of which email submission approach is used, CISA would be required to establish and implement processes to transfer data from the email submissions into an online case management system so that CIRCIA Reports submitted via email could be consolidated, analyzed, stored, etc., in a similar way as CIRCIA Reports submitted via the web-form or other subsequently approved mechanisms. These additional activities are likely to result in significant additional implementation costs for CISA, increase the amount of time it takes for CISA to receive necessary details about cyber incidents and ransom payments, and introduce an additional vector for error during the transcription or conversion of the data.

Third, email generally is not a secure form of transmission. Using unsecured email would increase the likelihood that an individual outside of the covered entity and CISA could gain access to potentially sensitive information on the covered cyber incident or ransom payment being reported, especially if the threat actor has compromised the covered entity's email system. CISA also would not be able to ensure that email submissions are protected at the level required by 6 U.S.C. 681e. Another challenge is the potential security concerns associated with receiving an email attachment from an entity that is compromised at the time of sending the email. CISA would be unable to guarantee the safety of the attachment and could be opening itself up to a security risk by accepting the email. Security measures CISA may implement to protect itself from such risks, as well as cybersecurity measures CISA has in place as a matter of routine, have the potential to block an email or attachment from making it to CISA, creating the possibility that a covered entity could take all steps intended to comply with their reporting obligation with CISA not receiving the CIRCIA Report.

Given these significant operational challenges, potentially substantial additional costs, and limited benefit associated with email submission above other options, CISA is not proposing email as a submission option at this time.

c. Fax

A fourth potential mechanism for covered entities to submit CIRCIA Reports would be via fax, which could be done by completing a report on paper and submitting it to CISA via fax machine or by submitting a fax electronically via an online faxing service or application. The primary benefit of offering faxing as a means of submission is that for many organizations, fax machines are separate from an organization's IT systems and thus may be available even when a cyber incident renders reporting via a web-based form or company email system unavailable. This benefit is somewhat limited these days, however, as fewer entities maintain actual fax machines as a means of communications, and online faxing services or applications are presumably no more likely to be an available and secure mechanism for an entity experiencing a cyber incident than reporting via a web-based form or company email system.³⁵²

Moreover, much like with email submissions, CIRCIA Reports submitted via fax would not provide a means for CISA to ensure that all required information is provided at the time of the submission. Consequently, CISA expects this could result in a large number of cases where CISA would need to follow up with the covered entity to obtain required information or validate the information received (*e.g.*, in the event that handwriting is illegible). CISA also would have to manually review and upload all submissions into an online case management system so that CIRCIA Reports submitted via fax could be consolidated, analyzed, stored, etc. in a similar way as CIRCIA Reports submitted via the web-form or other approved submission mechanisms. These additional activities are likely to result in additional implementation costs for CISA, increase the amount of time it takes for CISA to receive necessary details about the cyber incident or ransom payment, and introduce an additional vector for human error during the transcription or conversion of the data. Finally, faxing is generally considered insecure, with outdated protocols, and data that is

typically transmitted without encryption.³⁵³ For these reasons, CISA is not proposing faxes as a means for submitting CIRCIA Reports.

d. U.S. Mail or Other Physical Delivery Service

Another potential means for covered entities to submit CIRCIA Reports could be the delivery of physical, written reports using the U.S. Mail or other physical delivery service (*e.g.*, United Parcel Service, Federal Express, or a local courier). While this approach has the potential benefit of remaining available when a covered entity's information systems have been rendered unavailable or insecure due to the reportable incident, there are significant drawbacks associated with this mechanism of submission that likely would outweigh any associated benefits. Chief among these is the significant increase in the amount of time it likely would take for CISA to physically receive the submission from the covered entity. Depending on the service and postage used, it can take days for something sent via U.S. Mail or other delivery services to arrive at its destination. Even if overnight delivery service or local courier services were used, items delivered to a Federal agency such as CISA typically have to undergo security screening that frequently delays delivery to the intended office. These resulting delays could significantly impact the ability of CISA to achieve some of its statutory requirements, such as providing appropriate entities with timely, actionable, and anonymized reports of cyber incident campaigns and trends and immediately reviewing certain reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders. See 6 U.S.C. 681a(a)(3)(B), 681a(a)(7).

Much like with email and fax submissions, mail submission also does not provide a means for CISA to ensure that all required information is provided at the time of the submission. Consequently, CISA expects this would result in a number of cases where CISA would need to follow up with the covered entity to obtain required information. CISA also would have to manually review and upload all submissions into an online case management system so that CIRCIA Reports received by mail could be consolidated, analyzed, stored, etc. in

similar way as all other CIRCIA Reports. These additional activities are likely to result in significant additional implementation costs for CISA, increase the amount of time it takes for CISA analysts to receive necessary details about the cyber incident or ransom payment, and introduce an additional vector for human error during the transcription or conversion of the data. For these reasons, CISA is not proposing U.S. Mail or similar delivery services as an acceptable mechanism for submitting CIRCIA Reports.

e. Automated/Machine-to-Machine Reporting

Automated (*i.e.*, machine-to-machine or application programming interface (API)-based) reporting presents many potential benefits. If designed properly, automated reporting could provide nearly real-time, secure reporting of high volumes of incidents, in a manner and format tailored for analysis and incorporation into CISA's online case management system. Automated reporting could assure the use of consistent terminology and reduce the potential introduction of human error by eliminating the need for humans to enter or transcribe the data.

Automated cyber incident and ransom payment reporting does, however, potentially present some significant challenges. These challenges include potentially significant upfront costs to design a system and develop the associated standard; the costs for users to implement the standard, including any costs necessary to integrate it with their existing systems to feed the data exchange; and potentially significant amounts of overreporting if the automated reporting thresholds are not set properly by the covered entity.

Given the potentially significant benefits that could result from automated reporting, and the success that some other Federal regulators have had with automated reporting, this is an approach that CISA would be interested in exploring further once the CIRCIA final rule is issued and all necessary systems to support CIRCIA Reports are developed and deployed. CISA can envision this becoming an additional manner of submission approved by the Director in the future. At this time, however, CISA is not proposing automated reporting as a means for submission of CIRCIA Reports for a few reasons. First, CISA believes it is prudent to focus the finite technical and financial resources CISA has available for CIRCIA implementation on the development of the user-friendly, web-based form which CISA is required to offer as a means for submission of

³⁵² See, *e.g.*, Ashifa Kassam, *The Outdated Machine Hampering the Fight Against Covid-19*, BBC Future (Sept. 5, 2021) ("By 2000, fax's role in business was declining as companies switched to email and the internet to share information. But in other sectors, such as healthcare and real estate, the fax machine has stubbornly clung on."), available at <https://www.bbc.com/future/article/20210903-how-covid-19-could-finally-be-the-end-of-the-fax-machine>.

³⁵³ See, *e.g.*, Lily Hay Newman, *Fax Machines Are Still Everywhere, and Wildly Insecure*, Wired (Aug. 12, 2018), available at <https://www.wired.com/story/fax-machine-vulnerabilities/>.

CIRCI Reports. Second, until the rule is finalized and reporting begins, CISA will not know definitively the volume of reports CISA will be receiving or the number of covered entities that might be interested in using machine-to-machine reporting to comply with CIRCI. Prior to expending potentially significant resources on the development of machine-to-machine reporting capabilities, CISA would want to better understand the utility and demand for such a reporting mechanism and the potential return on investment of offering it as a means of reporting.

f. In-Person Reporting

One other method CISA considered is in-person reporting, either verbally or through provision of a written report, to a CISA staff member, such as a CISA Cybersecurity Advisor, Protective Security Advisor, Chemical Security Inspector, or a member of CISA's Cybersecurity Threat Hunting team. All of these individuals are trained security professionals who work daily with owners and operators of entities within the critical infrastructure sectors.

In-person reporting would have the benefit of facilitating direct engagement between an entity experiencing a cyber incident and CISA staff who might not only be able to receive a report, but also provide or direct the covered entity to assistance in responding to or mitigating the impacts of the incident. Direct engagement between CISA and the entity experiencing the incident may also help ensure that the most pertinent information is provided to CISA, and CISA may be able to get clarifications or answers to follow-up questions in real time, particularly for verbal reporting. In-person provision of a written report would also revert some of the downsides of mail-in reporting, such as by ensuring timeliness and real-time confirmation of receipt by CISA.

The downsides of in-person reporting include the increased burden required to broadly train CISA staff on the protocols for receiving in-person reports, the need for the individual receiving the report to subsequently input the information received into CISA's online case management system, and the additional likelihood of human error that these engagements would add into the process (though perhaps moderately less so than with telephone reporting as the parties could review the transcribed report with the reporting individual in real time). There also are logistical challenges that likely would limit the utility of this option as it would require the reporting individual and the CISA representative to be in the same physical location. This approach

would almost certainly require either a representative of a covered entity to travel to meet the CISA representative or vice versa, both delaying the time before reporting could be completed and increasing the cost of reporting (due to both the direct costs of travel and the indirect wage-related costs of the individual required to travel). Additionally, at least for verbal reporting, the CISA staff most likely to receive in-person reports are highly trained security professionals whose jobs are to engage with owners and operators of critical infrastructure. As these individuals already have significant, important day-to-day responsibilities, receiving and uploading CIRCI Reports may not be the most cost-efficient use of their taxpayer-funded time in support of CISA's mission. In light of these drawbacks, CISA is not proposing to use direct, in-person reporting as a mechanism for receiving CIRCI Reports.

ii. Form for Reporting

Section 681b(a)(6) of title 6, United States Code, states that Covered Cyber Incident Reports, Ransom Payment Reports, and Supplemental Reports "shall be made in the manner and form . . . prescribed in the final rule." As discussed in the previous section, CISA is proposing to use the "concise, user-friendly web-based form" CISA is required by 6 U.S.C. 681b(c)(8) to offer as a means for submission as the primary authorized means for submitting CIRCI Reports. CISA proposes naming this web-based form the "CIRCI Incident Reporting Form."

For the reasons discussed below, CISA is proposing to use the same user interface for the CIRCI Incident Reporting Form regardless of which of the four types of discrete mandatory reports identified in CIRCI (*i.e.*, Covered Cyber Incident Report; Ransom Payment Report; Joint Covered Cyber Incident and Ransom Payment Report; and Supplemental Report) that must be submitted by a covered entity. Additionally, CISA is proposing to use the same user interface regardless of whether a covered entity itself is submitting a CIRCI Report or if a third party is submitting a report on behalf of a covered entity. To facilitate this approach, CISA is proposing to use a dynamic, user-friendly, web-based form with conditional logic filters, with questions that adjust based on the answers to gateway or filtering questions used throughout the form. For instance, an early question might ask the submitter to indicate what type of report is being submitted—*e.g.*, a

Covered Cyber Incident Report, a Ransom Payment Report, a Joint Covered Cyber Incident and Ransom Payment Report, a Supplemental Report—and the questions that follow will be tailored based on the response provided by the submitter.

CISA believes that numerous benefits exist in using the same user interface for all CIRCI Reports (and potentially for voluntarily provided reports as well). First, this approach would allow all entities to go to a single location to comply with their CIRCI reporting obligations regardless of what type of CIRCI Report they need to submit. Second, it would prevent the covered entity from having to choose from multiple different forms to determine which is the correct set of questions for their particular reporting situation. There are a variety of circumstances under which a covered entity may be submitting a CIRCI Report, such as a covered cyber incident that does not involve a ransom payment, a covered cyber incident for which a ransom payment has been made, a ransom payment being reported via a Supplemental Report after a covered cyber incident has been submitted, or a ransom payment made in response to a cyber incident that does not meet the criteria of a covered cyber incident. Instead of creating unique forms for each possible reporting scenario and requiring the covered entity to correctly identify which one applies, having a single user interface that can be used to address any potential reporting circumstance eliminates both the need for the covered entity to expend resources identifying the correct form and the possibility of the covered entity selecting the incorrect form.

Finally, a single user interface also reduces the burden in situations where the covered entity's reporting requirements change during the preparation of the report. For instance, a covered entity may begin to report a covered cyber incident and, before submitting it to CISA, the entity makes a ransom payment as part of its response to the incident. Having a dynamic user interface may make it possible to allow the covered entity to modify its responses to certain questions and/or add the additional information related to the ransom payment rather than recreate all of its previous work in a separate form designed specifically for submitting a Joint Covered Cyber Incident and Ransom Payment Report.

The dynamic nature of the concise, user-friendly, web-based form being proposed by CISA has additional benefits beyond the facilitation of a single form model. A dynamic user

interface supports the tailoring of questions even within a single type of report (e.g., a Covered Cyber Incident Report), allowing CISA to present only those secondary or tertiary questions applicable to the covered entity's unique circumstances, thus minimizing the overall number of questions asked of each submitter.³⁵⁴ Similarly, in addition to appropriately modifying whether a question is asked at all, a dynamic approach also allows CISA to vary whether responding to specific questions is required or optional based on the report type and other answers provided by the submitter.

In the user interface, CISA intends to use a mixture of input options, such as radio buttons, drop-down menus, and text boxes. Tailoring the response format and options for individual questions will allow CISA to advance various goals simultaneously, to include reducing the burden of completing the report, supporting consistency in terminology to facilitate analysis of data, facilitating the logic-flow based tailoring of questions, and offering opportunities for covered entities to provide additional pertinent details via narratives where useful.

As discussed in the previous section, CISA intends to maintain the ability to receive telephonic reports as a back-up option and, in the future, may offer alternative mechanisms for a covered entity to submit a report beyond the web-based user interface, such as automated (*i.e.*, machine-to-machine) reporting. If CISA offers, and a covered entity elects to use, a mechanism other than the web-based user interface to submit a report, CISA will establish procedures to ensure all mandatory questions are answered and the benefits of a single, dynamic form are preserved to the maximum extent practicable. For example, if CISA were to allow telephonic reporting in the future, CISA could have an operator complete the web-based form for the caller by verbally talking the caller through the form, asking them every pertinent question, typing the responses into the form, and then transmitting the covered

³⁵⁴ For instance, for a hypothetical first-level question on what type of entity a covered entity is (e.g., individual, corporation, State or local government), a covered entity that indicates it is a State or local government might receive a secondary question asking it to identify what State it represents and a tertiary question asking it to identify the State department or agency. If the covered entity instead indicated it was a corporation, it would not be asked those specific secondary or tertiary questions, but rather might be asked different questions that would not be visible to an entity that indicated it was a State or local government, such as the State in which the corporation was incorporated and the corporation's Data Universal Numbering System (DUNS) number.

entity a copy of the completed report for its records. Similarly, if a fillable PDF or paper-based format is offered, CISA could design that paper-based form in a manner similar to forms used by the Internal Revenue Service for filing of taxes, where the provision of specific answers to questions on the universal section of the form direct the preparer of the form to annexes or addendums that they should complete and include with their submission given their case-specific circumstances.³⁵⁵

Consistent with what has been discussed above, 6 U.S.C. 681b(a)(5)(A) requires that CISA offer a means to comply with reporting requirements for both a covered cyber incident and a ransom payment using a single report if a covered entity makes a ransom payment prior to the 72-hour requirement for submitting a Covered Cyber Incident Report.³⁵⁶ CISA's proposed approach of using a dynamic reporting user interface for all CIRCIA Reports would enable a covered entity to submit information on both a covered cyber incident and ransom payment at the same time using the same form, thus satisfying this statutory requirement. As discussed in Section IV.A.iii.4 in this document, CISA is proposing to call this report a Joint Covered Cyber Incident and Ransom Payment Report. To complete this type of report, a covered entity should follow the processes described herein that apply to all CIRCIA Reports and include all content required in both a Covered Cyber Incident Report and Ransom Payment Report, as set out in the following section and §§ 226.7 through 226.10 of the proposed regulation.

iii. Content of Reports

Sections 681b(c)(4) and (5) of title 6, United States Code, require CISA to include in the final rule a "clear description of the specific required contents" of a Covered Cyber Incident Report and Ransom Payment Report, respectively. Sections 226.7 through

³⁵⁵ For example, an individual only needs to complete Schedule B to Form 1040 if they received certain interest or ordinary dividends during a given tax year (see <https://www.irs.gov/forms-pubs/about-schedule-b-form-1040> (last visited Nov. 28, 2023)) or Schedule C if they need to report income or loss from a business operated or profession practiced as a sole proprietor (see <https://www.irs.gov/forms-pubs/about-schedule-c-form-1040> (last visited Nov. 28, 2023)).

³⁵⁶ Specifically, 6 U.S.C. 681b(a)(5)(A) states "If a covered entity is the victim of a covered cyber incident and makes a ransom payment prior to the 72 hour requirement under paragraph (1), such that the reporting requirements under paragraphs (1) and (2) both apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the final rule issued pursuant to subsection (b)."

226.11 of the proposed regulation contain a description of the content required in those reports, as well as the other two types of CIRCIA Reports.

In determining what content covered entities should be required to include in either a Covered Cyber Incident Report or Ransom Payment Report, CISA considered a variety of sources. First and foremost, CISA considered 6 U.S.C. 681b(c)(4) and (5), as those sections contain extensive lists of the specific types and categories of information that submitters must include in Covered Cyber Incident Reports and Ransom Payment Reports, respectively.

Second, CISA examined what data is required for CISA to perform the activities Congress assigned to CISA within CIRCIA and evaluated whether that data is captured within the content categories enumerated in 6 U.S.C. 681b(c)(4) and (5). Based on that evaluation, CISA determined that certain data CISA will need to perform its statutory mandates will not necessarily be captured by any of the categories of content specified by Congress in 6 U.S.C. 681b(c)(4) and (5). Accordingly, CISA is proposing to make that content required in one or more types of CIRCIA Report. For example, 6 U.S.C. 681a(a)(3)(B) of CIRCIA requires CISA to "provide appropriate entities . . . with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including . . . related contextual information, cyber threat indicators, and defensive measures." To comply with this requirement, CISA needs to collect information on cyber threat indicators from victims of cyber incidents. Accordingly, while some of the categories enumerated in 6 U.S.C. 681b(c)(4) and (5) would likely elicit the submission of some information that would qualify as cyber threat indicators (as defined in 6 U.S.C. 650(5)), CISA is proposing including additional mandatory content for CIRCIA Reports for CISA to collect a broader range of cyber threat indicators.

Third, CISA engaged with stakeholders from across the Federal government to determine what data related to cyber incidents might be useful to them to accomplish their respective missions or, for those with their own cyber incident reporting programs, what data they have found to be the most useful and other information that might be helpful to have in the future. Among the groups CISA consulted were:

- the SRMAs responsible for coordinating critical infrastructure security efforts across the 16 critical infrastructure sectors;

- members of the law enforcement and intelligence communities, such as the Federal Bureau of Investigation (FBI), the U.S. Secret Service, the Department of the Treasury's Financial Crimes Enforcement Network, and the NSA; and

- Federal departments and agencies that oversee cyber incident reporting regulations or directives, such as DOE, NRC, SEC, FCC, TSA, and the Department of the Treasury's OCC.

In this vein, CISA also considered what incident-related information CISA has found to be the most useful in executing non-CIRCIAs responsibilities, including CISA's asset response authorities under 6 U.S.C. 652(c)(1) and 659(f)(1) and as further described in Presidential Policy Directive—41, *United States Cyber Incident Coordination*.

CISA also solicited the perspective of the public and members of the private sector on this topic through the issuance of an RFI and the hosting of more than two dozen listening sessions. CISA received numerous comments on contents of reports, which have been considered by CISA in developing the proposed content of reports. More information on the comments received by CISA in response to the RFI and during the CIRCIAs listening sessions can be found in Section III.F in this document.

Finally, CISA reviewed the Model Reporting Form developed by DHS through the CIRC effort. As part of the CIRC's mandate to promote harmonization of Federal cyber incident reporting regulations and minimize the burden on entities that may need to comply with more than one cyber incident reporting requirement, DHS, informed by close collaboration with the CIRC, developed a Model Reporting Form. CISA fully supports harmonizing cyber incident reporting requirements where practicable and has sought to align the CIRCIAs reporting form required content with the content recommendations in the Model Reporting Form where practical and consistent with the CIRCIAs statutory requirements related to both the content of CIRCIAs Reports and CISA's obligations with respect to information received through CIRCIAs Reports.

Based on the above, CISA is proposing certain content be submitted by a covered entity regardless of the type of CIRCIAs Report being submitted, while other content will be required only in certain types of CIRCIAs Reports. The following subsections discuss the categories of content that CISA is proposing be required for inclusion in (a) all CIRCIAs Reports, (b) Covered

Cyber Incident Reports (and subsequent Supplemental Reports as necessary) only, (c) Ransom Payment Reports only, and (d) Supplemental Reports only.

1. Proposed Content To Be Included in All CIRCIAs Reports

This subsection describes the content, such as contact information for the covered entity, that CISA is proposing must be included regardless of the type of CIRCIAs Report a covered entity is submitting. Other categories of content that CISA is proposing for inclusion in a specific type of report, such as the date and amount of the ransom payment, follow, organized by report type.

The majority of the content proposed for inclusion is explicitly required by CIRCIAs. Where this is the case, the discussion below will include a reference to the specific statutory provision in CIRCIAs requiring the inclusion of the proposed content. Where CISA is proposing to seek content beyond what is explicitly set out in 6 U.S.C. 681b(c)(4) and (5), the rationale supporting that proposal is included.

a. Report Type

At or near the beginning of the reporting user interface will be questions related to what type of report an entity wants to submit. This will help identify if a report is a Covered Cyber Incident Report, a Ransom Payment Report, a Joint Covered Cyber Incident and Ransom Payment Report, or a Supplemental Report. The answer submitted in response to these questions will help determine the spectrum of additional content the reporting entity will be asked to provide and may be used to streamline reporting in other ways, such as by supporting the pre-population of previously submitted data when submitting a Supplemental Report, to the extent pre-population is available for the covered entity's chosen manner of submission. This section of the form also may include some optional questions such as whether this information is being additionally submitted to meet any other reporting requirements. If a covered entity is reporting an incident to CISA per another regulatory requirement and intends for this report to also meet its reporting obligations under CIRCIAs, the covered entity would need to indicate both requirements on the form. Otherwise, a separate CIRCIAs Report would need to be filed.

b. Identity of the Covered Entity

All CIRCIAs Reports are statutorily required to include information

sufficient to clearly identify the c making the report or on whose behalf the report is being made. See 6 U.S.C. 681b(c)(4)(E) and (5)(D). This must include, as applicable, the State of incorporation or formation of the covered entity, trade names, legal names, or other identifiers. See 6 U.S.C. 681b(c)(4)(E) and (5)(D). Other types of information that CISA intends on requesting in this section of the form include the entity type (e.g., Federal, State, local, Territorial, Tribal, ISAC, private sector); physical address; organization's website; any internal incident tracking number used by the entity for the reported event (if one exists); any applicable business numerical identifiers, such as a NAICS code, General Services Administration-Issued Unique Entity Identifier (GSA-UEI), Dun & Bradstreet Data Universal Numbering System (D-U-N-S) Number, Tax ID Number, EPA Facility ID number; Chemical Security Assessment Tool (CSAT) ID Number, or MTSA Facility ID Number; the name of the covered entity's parent corporation or organization, if applicable; and the critical infrastructure sector or sectors of which the covered entity considers itself a part. This additional information will help ensure that CISA has the correct identity of the covered entity (including understanding the corporate familial relationship between the covered entity or covered entities that experienced the substantial cyber incident and any subsidiary, parent, or sister corporation or organization that may be reporting on behalf of affected subsidiaries, parents, or sisters), facilitate information sharing with appropriate partners, and support trend and threat analysis by specific geographic regions, entity types, critical infrastructure sectors, and other characteristics.

c. Contact Information

All CIRCIAs Reports are statutorily required to include contact information, such as telephone number or email address, that CISA may use to contact the covered entity, an authorized agent thereof, or, where applicable, an authorized third party acting with the express permission and at the direction of the covered entity to assist with compliance with CIRCIAs reporting requirements. 6 U.S.C. 681b(c)(4)(F) and (5)(E). To satisfy this statutory requirement, CISA is proposing requiring a covered entity to provide the name, phone number, email, and title of the reporting party and, if different, the point of contact for the covered entity. CISA is also proposing requiring a covered entity to provide the name, phone number, email address, and title

of the covered entity's registered agent, if that individual is different than the identified point of contact. CISA also is proposing that in cases where a third party is submitting a report on behalf of a covered entity, the aforementioned contact information must be provided for both the third-party submitter and the covered entity point of contact.

CISA additionally is proposing to include an optional field through which contact information for a 24/7 point of contact could be provided to better enable incident response support and emergency follow-up engagement. CISA may also include optional fields for additional contact information elements such as a classified phone number or classified email account where the 24/7 point of contact or another identified individual(s) can be reached, if applicable.

d. Third Party Authorization To Submit

Pursuant to 6 U.S.C. 681b(d)(1), a covered entity may use a third party to submit a CIRCIA Report on behalf of the covered entity. As discussed in greater detail in Section IV.E.v.3.a in this document, CISA is proposing requiring a third party that submits a report on behalf of a covered entity to include in the submission an attestation that it has been expressly authorized by the covered entity to submit the report. CISA is proposing to require this indication of authorization in any CIRCIA Report submitted by a third party on behalf of a covered entity, regardless of the type of report. This requirement is set forth in § 226.7(d) of the proposed regulation. Additional details on third-party submissions and the proposed requirement for third-party submitters to confirm their authority to submit a CIRCIA Report on a covered entity's behalf can be found in Section IV.E.v.3 in this document.

2. Covered Cyber Incident Report Specific Content

CISA is proposing requiring submission of information in the following categories of content in a Covered Cyber Incident Report. As noted in the individual content categories, CISA is proposing that some of the proposed data elements within the individual content categories are required while other proposed data elements are optional. CISA intends to ask for all the required information in an initial Covered Cyber Incident Report; however, CISA understands that a covered entity may not know all of the required information within the initial 72-hour reporting timeframe. Accordingly, answers of "unknown at this time" or something similar will be

considered acceptable for certain questions in initial reporting. A covered entity must, however, comply with its Supplemental Reporting requirements and provide previously unknown information promptly to CISA once discovered if the information meets the "substantial new or different information" threshold. That includes any information required to be submitted in an initial Covered Cyber Incident or Joint Covered Cyber Incident and Ransom Payment Report that a covered entity subsequently learns after initially responding that the information was unknown at the time of reporting. See Section IV.E.iv.3.b in this document for a more fulsome discussion on what CISA is proposing constitutes "substantial new or different information." CISA is proposing that a covered entity ultimately must provide all applicable required content in either the initial Covered Cyber Incident Report or a Supplemental Report to be considered fully compliant with its reporting obligations under CIRCIA.

a. Description of the Covered Incident

The first category of content required by CIRCIA is focused on ensuring CISA receives information on the systems affected by the incident and the impacts of the incident. Specifically, 6 U.S.C. 681b(c)(4)(A) requires covered entities to include in a Covered Cyber Incident Report a "description of the covered cyber incident" containing, among other things, an identification and description of the affected information systems, networks, or devices; a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations; the estimated date range of the incident; and the impact to the operations of the covered entity. To collect this information, CISA is proposing including a combination of one or more text boxes where entities can provide a narrative description of the incident or specific aspects of the incident along with a series of questions containing radio buttons, drop-down menus, or limited data fields (e.g., dates) to ensure the provision of certain information.

For the first statutorily enumerated element under this category—identification and a description of the function of the affected information systems, networks, or devices—CISA is interested in the name and a description of the impacted systems, networks, and/or devices, to include technical details and physical locations of the impacted systems, networks, and/or devices. CISA

also would like to know if any of the impacted systems, networks, and/or devices contain or process information created by or for any element of the Intelligence Community or contain information that has been determined by the United States Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in 42 U.S.C. 2014(y).

For the second statutorily enumerated element under this category—description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations—CISA is interested in whether the incident involved any unauthorized access (whether or not the access involves an attributed or unattributed cyber intrusion), whether there were any informational impacts, or whether any information was compromised. If the answer to any of those questions is "yes," CISA proposes requiring the covered entity to answer a small number of follow-up questions to elicit additional details. CISA also intends to request information regarding what network location(s) the activity was observed in. While the statutorily enumerated element incorporates the "substantial loss" standard from the first prong of the definition of substantial cyber incident, CISA is proposing to require covered entities to describe any unauthorized access once an incident meets the reportable threshold so that CISA and other Federal agencies can have a broader understanding of potential impacts to the CIA of information systems, networks, or the information therein. CISA believes the "disruption of business or industrial operations" portion of this statutorily enumerated element is sufficiently addressed by the fourth statutorily enumerated element, discussed below.

For the third statutorily enumerated element under this category—incident date range—CISA is proposing to seek information on the date the covered cyber incident was detected, the date the covered cyber incident began (if known), the date the covered cyber incident was fully mitigated and resolved (if it has been), and the timeline of compromised system communications with other systems. For incidents involving unauthorized access, CISA also proposes asking about the suspected duration of the unauthorized access prior to detection and reporting. While CISA is proposing

to ask for more details than just the incident date range (*i.e.*, the beginning and end of the incident), understanding the key timeline of events that comprised the incident is key to enhancing the Federal government's understanding of the incident as a whole.

In describing this category of information, the proposed regulatory text refers to the incident as the "covered cyber incident" to refer to the incident that is subject to the CIRCIA reporting requirement. CISA does not interpret the use of that term to import any threshold definitional triggers. For example, in requiring that the Covered Cyber Incident Report include the date that the covered cyber incident began, CISA is not asking for the date on which the covered entity began experiencing impact levels that met the definition of a substantial cyber incident, and therefore a covered cyber incident. Rather, once a covered entity has determined it has experienced a covered cyber incident, it should report all relevant dates related to the underlying cyber incident. As such, the date that the covered cyber incident began would be the earliest date of identified unauthorized activity associated with the cyber incident that would ultimately become the covered cyber incident.

For the final statutorily enumerated element under this category—impacts to the operations of the covered entity—CISA proposes asking various questions to understand both the level of impact and specific impacts, such as whether any known or suspected physical or informational impacts occurred. CISA is also proposing to include questions related to the nature of the impact, *i.e.*, was the system, network, device, or data accessed, manipulated, exfiltrated, destroyed, or rendered unavailable. To satisfy some of the requirements imposed upon CISA by CIRCIA, CISA also needs information on impacts of the incident beyond simply the operations of the covered entity. For instance, among other things, 6 U.S.C. 681a(a) requires CISA to analyze Covered Cyber Incident Reports to assess potential impacts of cyber incidents on public health and safety. Similarly, 6 U.S.C. 681a(c) requires CISA to periodically brief certain members of Congress on the national cyber threat landscape. Likewise, 6 U.S.C. 681a(a)(6) requires CISA to review any covered cyber incidents or group of incidents that are likely to result in demonstrable harm to the economy of the United States and identify and disseminate ways to prevent similar incidents in the future. In support of these and other

requirements, CISA also envisions asking questions that will help CISA assess the economic impacts of the incident and the potential impacts of the incident on public health and safety, national security, economic security, and any of the NCFs.

CIRCIA also requires a covered entity to include in its Covered Cyber Incident Report the "category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person." 6 U.S.C. 681b(c)(4)(D). CISA proposes including questions related to this topic in the Covered Cyber Incident Report form.

b. Vulnerabilities, Security Defenses, and TTPs

The second statutorily required block of content is focused on how the incident was carried out. Specifically, 6 U.S.C. 681b(c)(4)(B) requires covered entities to include in a Covered Cyber Incident Report "[w]here applicable, a description of the vulnerabilities exploited and security defenses in place, as well as the tactics, techniques, and procedures used to perpetrate the covered cyber incident." This information will enable CISA to carry out its core statutory responsibilities related to identifying and sharing information on cyber incident trends, TTPs, vulnerability exploitations, campaigns, and countermeasures that may be useful in preventing others from falling victim to similar incidents and preventing similar vulnerability classes in the future.

CISA is proposing to codify the need to submit information to address this statutory requirement in five consecutive regulatory subsections. First, proposed § 226.8(c) would require the submission of information on the vulnerabilities exploited, including but not limited to the specific products or technologies and versions in which the vulnerabilities were found. Next, proposed § 226.8(d) would require the submission of information on the covered entity's security defenses, including but not limited to any controls or measures that resulted in detection or mitigation of the incident. As part of this, CISA is likely to ask what, if any, security controls or control families (*e.g.*, NIST Special Pub 800–171 controls³⁵⁷; NIST Cybersecurity Framework measures³⁵⁸; CISA

Cybersecurity Performance Goal activities³⁵⁹) the covered entity had in place on the compromised system, and, to the extent known, which controls or control families failed, were insufficient, or not implemented that may have been a factor in this incident. CISA also is likely to include questions aimed at helping CISA understand how the covered entity identified the incident; what, if any, detection methods were used to discover the incident; and if the covered entity has identified the initially affected device(s).

Finally, proposed § 226.8(e), (f) and (g) would require information on the type of incident (*e.g.*, denial-of-service; ransomware attack; multi-factor authentication interception); the TTPs used to cause the incident, to include any TTPs that were used to gain initial access to the covered entity's system; indicators of compromise observed in connection with the covered cyber incident; and a description and copy or sample of any malicious software the covered entity believes is connected with the covered cyber incident. Questions CISA may ask to obtain this information potentially include what, if any, attack vectors did the covered entity identify; to the covered entity's knowledge, were any advanced persistent threat actors involved; were any malicious software, malicious scripts, or other indicators of compromise found, and, if so, what specific variants or strains were used. In addition to a description of any malware samples or indicators of compromise observed or captured by the covered entity, CISA is proposing to require covered entities provide indicators of compromise identified as well as copies of any malware samples related to the covered cyber incident that the covered entity has in its possession. While 6 U.S.C. 681b(c)(4)(B) uses the term "description," obtaining actual indicators of compromise and copies of malware samples, rather than a mere description, is important to enable CISA to perform the activities assigned to CISA under CIRCIA (including identifying, developing, and disseminating actionable cyber threat indicators and defensive measures), and is also consistent with key requests in other incident reporting programs.³⁶⁰

³⁵⁹ See CISA, *Cross-Sector Performance Goals*, available at <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>.

³⁶⁰ See, *e.g.*, 48 CFR 252.204–7012(d) (requirement in DFARS incident reporting requirement for contractors to submit copies of malicious software to DOD when they have

³⁵⁷ See NIST, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST Special Publication 800–171 Rev. 2, (Feb. 2020), available at <https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final>.

³⁵⁸ See NIST, *Cybersecurity Framework 2.0*, available at <https://www.nist.gov/cyberframework>.

In cases where the covered cyber incident involves a ransomware attack but the covered entity did not make a ransom payment and is thus not obligated to submit a Ransom Payment Report, pursuant to proposed § 226.8(e), CISA intends to ask specific questions related to ransomware attack-specific TTPs, such as information on the ransom payment demand and instructions, that a covered entity would otherwise have been required to provide in a Ransom Payment Report were one required. This information will help CISA and its partners on the Joint Ransomware Task Force established pursuant to CIRCIA more fully understand and combat existing threats related to ransomware attacks.

To assist in the development of responses to these questions and the use of common terminology, CISA anticipates providing drop-down menus or other selection options tied to the MITRE ATT&CK® framework³⁶¹ or another broadly recognized cyber incident reporting framework. CISA may also ask whether the entity has any applicable logs (e.g., network logs; system logs; memory captures) available.

CISA recognizes that some of the information requested in this section of the form may be unavailable at the time a covered entity is submitting the initial Covered Cyber Incident Report. Nevertheless, to assist CISA in conducting analysis and providing early warnings in as timely a manner as possible, CISA does intend to ask for this information in Covered Cyber Incident Reports and expects covered entities to provide that information when they possess it with some degree of confidence; however, good faith answers of “unknown at this time” or something similar generally will be acceptable responses to these questions in an initial Covered Cyber Incident Report. If this information is not submitted in the initial report, to the extent the information is applicable to the incident and knowable, a covered entity will be required to include that information in a Supplemental Report before its reporting obligations are considered met under the regulation. A covered entity should keep in mind its obligation to report “substantial new and different information” to CISA “promptly” upon discovery and should not be waiting until all unknown information is gathered before

discovered and isolated malicious software in connection with a reported cyber incident).

³⁶¹ MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations, available at <https://attack.mitre.org/>.

submitting a Supplemental Report to CISA.

c. Information Related to the Identity of the Perpetrator of the Incident

Section 681b(c)(4)(C) of title 6, United States Code, requires covered entities to include in a Covered Cyber Incident Report “[w]here applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such cyber incident.” CISA is proposing to include in this section questions seeking any attribution-related information the covered entity may possess. Additionally, CISA is proposing to include in this section questions regarding whether the covered entity believes they can attribute the cyber incident, what evidence supports their attribution assessment, and how confident they are in their attribution assessment.

d. Mitigation/Response

Although not included among the specifically required contents enumerated in 6 U.S.C. 681b(c)(4), CISA is proposing a small number of questions regarding the mitigation and response activities a covered entity is taking or has taken in response to a covered cyber incident. Under 6 U.S.C. 681a(a)(3)(B) and (7), CISA is required to, among other things, leverage information gathered about cyber incidents to provide appropriate entities with defensive measures, and, with respect to Covered Cyber Incident Reports involving an ongoing cybersecurity threat or security vulnerability, immediately review those reports and disseminate defensive measures. Further, under 6 U.S.C. 681a(a)(6), CISA is required to conduct a review of details surrounding each covered cyber incident or group of such incidents that satisfy the definition of a significant cyber incident to identify and disseminate ways to prevent or mitigate similar incidents in the future. Understanding the mitigation and response activities taken by a covered entity will be key to CISA’s ability to identify or develop defensive measures that can be leveraged by other entities, as well as to evaluate and identify ways to mitigate similar incidents in the future.

The questions CISA is proposing to ask to support this analysis include what mitigation measures the covered entity had in place, what responsive actions the covered entity has taken, what phase of incident response (e.g., detection, analysis, containment, eradication, recovery, and post-incident activity) the covered entity is currently

in, and what is the covered entity’s assessment of the efficacy of those mitigation and response activities.³⁶² As part of this, CISA is also proposing to ask about engagement with law enforcement agencies, if the covered entity reached out to another entity for mitigation or response assistance, and, if so, to whom.³⁶³ CISA will also provide an opportunity for the covered entity to indicate that it would like to request assistance from CISA related to the incident. This information will facilitate CISA’s coordination with its Federal partners, including law enforcement, and non-Federal partners who may already be engaged in responding to the incident.

e. Additional Data or Information

CISA is proposing to require a covered entity to include in a Covered Cyber Incident Report any other data or information required by the web-based CIRCIA Incident Reporting Form or other authorized manner and form of reporting. CISA recognizes that cyber incidents are dynamic in nature and that, over time, CISA may identify additional data or information that would be useful or necessary to meet the purposes of the CIRCIA regulations. CISA may also identify ways to streamline reporting in response to particular circumstances, such as by allowing covered entities to check a box to indicate if their Covered Cyber Incident Report is related to a specific known campaign, supply chain compromise, or compromise of a third-party service provider. CISA is proposing to include § 226.8(j) to ensure that covered entities would be required to include any additional required data or information that CISA subsequently determines is necessary and consistent with CISA’s authorities under CIRCIA. Additionally, CISA may include optional requests for data and information that apply to the type of covered cyber incident reported and that may help clarify the covered entity’s responses to information required by § 226.8. CISA is proposing to include similar language in § 226.9(n) for Ransom Payment Reports and

³⁶² See NIST, *Computer Security Incident Handling Guide*, NIST Special Publication 800–61 Rev. 2, at 21–45 (Aug. 2012), available at <https://csrc.nist.gov/pubs/sp/800/61/r2/final> (hereinafter “NIST SP 800–61r2”).

³⁶³ In response to this topic and the related topic in the required content for Ransom Payment Reports, covered entities do not need to include every vendor from whom they have sought a quote but did not ultimately use. However, covered entities should not necessarily limit their response to entities from whom they have actually received assistance, particularly as some requests for assistance may remain outstanding at the time the report is submitted.

§ 226.11(a)(4) for Supplemental Reports. CIRCIA exempts any action required to carry out 6 U.S.C. 681b, including the reporting requirements in 6 U.S.C. 681b(a)(1)-(3), from compliance with the PRA requirements codified in 44 U.S.C. 3506(c), 3507, 3508, and 3509. 6 U.S.C. 681b(f). This exemption includes actions taken by CISA to make changes to the questions included in the CIRCIA web-based Incident Reporting Form as described above and to solicit for optional information and data as part of CIRCIA Reports.

3. Ransom Payment Report Specific Content

Section 681b(c)(5) of title 6, United States Code, enumerates specific content that is to be included in a Ransom Payment Report. Two of the enumerated items, information identifying the covered entity that made the ransom payment (or on whose behalf the ransom payment was made) and contact information for the covered entity or an authorized agent thereof, were discussed previously and are part of the categories of information that must be included regardless of report type. The remaining items enumerated in 6 U.S.C. 681b(c)(5) are specific to Ransom Payment Reports and are discussed in the following subsections.

a. Description of the Ransomware Attack

Section 681b(c)(5)(A) of title 6, United States Code, requires a covered entity to include in its Ransom Payment Report a “description of the ransomware attack, including the estimated date range of the attack.” For those ransom payments that are the result of a covered cyber incident and for which a Covered Cyber Incident Report has been submitted, the information necessary to address this category will have been contained in the Covered Cyber Incident Report. For those ransom payments that are not the result of a covered cyber incident, or for which a Ransom Payment Report is being submitted prior to the submission of a Covered Cyber Incident Report, CISA is proposing requiring the covered entity to include in its Ransom Payment Report questions similar to those asked in § 226.8(a) of the regulation and described in Section IV.E.iii.2.a in this document. While 6 U.S.C. 681b(c)(4)(A) includes much more specific detailed requirements as to what must be included in a description of a covered cyber incident than the parallel 6 U.S.C. 681b(c)(5)(A) includes for the required description of ransomware attacks, CISA is proposing to ask similar questions for this topic because, for the reasons described in Section IV.E.iii.2.a in this

document, these questions would provide CISA with relevant information to understand the incident and its impact.

b. Vulnerabilities, Security Defenses, and TTPs

Section 681b(c)(5)(B) of title 6, United States Code, requires a covered entity to include in its Ransom Payment Report, “where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetrate the ransomware attack.” For those ransom payments that are the result of a covered cyber incident and for which a Covered Cyber Incident Report has been submitted, the information necessary to address this category will have been contained in the Covered Cyber Incident Report or a previously submitted Supplemental Report. For those ransom payments that are not the result of a covered cyber incident, or for which a Ransom Payment Report is being submitted prior to the submission of a Covered Cyber Incident Report, CISA is proposing requiring the covered entity to include in its Ransom Payment Report questions similar to those asked in § 226.8(c)–(f) of the regulation and described in Section IV.E.iii.2.b in this document. While 6 U.S.C. 681b(c)(5)(B) does not include reference to the security defenses, as is included in the parallel 6 U.S.C. 681b(c)(4)(B), CISA is proposing to ask similar questions about security defenses in Ransom Payment Reports. This information will enable CISA to carry out its core statutory responsibilities related to identifying and sharing information on cyber incident trends, TTPs, vulnerability exploitations, campaigns, and countermeasures that may be useful in preventing others from falling victim to similar incidents, and preventing similar vulnerability classes in the future, regardless of whether the ransomware attack that precipitated the ransom payment was a covered cyber incident or not. This information would be particularly useful to CISA in preventing others from falling victim to similar ransomware attacks that could rise to the level of being a covered cyber incident in the event those security defenses were the reason why a particular ransomware attack did not rise to the level of a substantial cyber incident.

c. Information Related to the Identification of the Perpetrator of the Attack

Section 681b(c)(5)(C) of title 6, United States Code, requires a covered entity to include in its Ransom Payment Report, “where applicable, any identifying or

contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.” For those ransom payments that are the result of a covered cyber incident and for which a Covered Cyber Incident Report has been submitted, the information necessary to address this category will have been contained in the Covered Cyber Incident Report. For those ransom payments that are not the result of a covered cyber incident, or for which a Ransom Payment Report is being submitted prior to the submission of a Covered Cyber Incident Report, CISA is proposing requiring the covered entity to include in its Ransom Payment Report questions similar to those asked in § 226.8(h) of the regulation and described in Section IV.E.iii.2.c in this document.

d. Information on the Ransom Payment

Sections 681b(c)(5)(F)–(I) of title 6, United States Code, require a covered entity to submit a variety of information related to any ransom payment it makes or that gets made on its behalf. This information includes the date of the ransom payment (6 U.S.C. 681b(c)(5)(F)); the ransom payment demand, including the type of virtual currency or other commodity requested (6 U.S.C. 681b(c)(5)(G)); the ransom payment instructions, including information regarding where to send the payment (6 U.S.C. 681b(c)(5)(H)); and the amount of the ransom payment (6 U.S.C. 681b(c)(5)(I)). CISA is proposing including questions in the Ransom Payment Report sufficient to elicit submission of these statutorily required data elements, including details to help contextualize these elements (such as the type of assets used in the ransom payment, which is necessary to understand the value of the amount of the ransom payment), as well as information useful to identify the completed transaction, such as any transaction identifier or hash.

To ensure completeness in the response and a full understanding of the ransom demand, CISA is proposing to require the covered entity to provide either the verbatim text of the demand or, where available, a screenshot or copy of the actual ransom demand. Additionally, if multiple demands were made during a single incident, CISA expects the covered entity to provide the required information on each such demand. Similarly, if multiple ransom payments were made in response to a single incident, a covered entity is required to report each such ransom payment.

e. Results of Ransom Payment

CISA is proposing to require a covered entity to include in a Ransom Payment Report information regarding what occurred as the result of the covered entity making the ransom payment. Examples of information that CISA would expect a covered entity to provide under this heading would be whether any data that had been exfiltrated was returned or, in cases where the perpetrator encrypted any of the covered entity's systems or information, whether a decryption capability was provided. If a decryption capability was provided, CISA would seek specific information on that capability, to include whether or not it was effective.

f. Additional Data or Information

CISA is proposing to require a covered entity to include in a Ransom Payment Report three additional items, all of which CISA is proposing to require in a Covered Cyber Incident Report as well. First, CISA is proposing to ask whether the covered entity requested assistance from another entity in responding to the ransomware attack or making the ransom payment and, if so, the identity of such entity or entities. This information will help CISA understand the capabilities covered entities typically do and do not possess to respond to a ransomware attack, where assistance may be beneficial, and the broader ecosystem of activities related to ransomware attacks. This will also help CISA have a better understanding of the universe of entities who may be subject to the responsibilities to advise a covered entity pursuant to § 226.12(d) (discussed further in Section IV.E.v.3.e in this document).

Second, CISA is proposing to require a covered entity to provide information on any engagement the covered entity has had with any law enforcement agency related to the ransom payment or underlying ransomware attack. Such information would be extremely beneficial to effective operations of the Joint Ransomware Task Force established by CIRCIA and help the Federal government minimize the potential for uncoordinated law enforcement activities.

Finally, CISA is proposing to require a covered entity to include in a Ransom Payment Report any other data or information required by the web-based CIRCIA Incident Reporting Form or any other authorized manner and form of reporting. Cyber incidents involving ransom payments are dynamic in nature and, over time, CISA may identify

additional data or information that would be useful or necessary to meet the purposes of CIRCIA. CISA is proposing to include § 226.9(n) to ensure that covered entities would be required to include any additional required data or information that CISA subsequently determines is necessary and consistent with CISA's authorities under CIRCIA. Additionally, CISA may include optional requests for data and information that may help clarify the covered entity's responses to information required by § 226.9. CISA is proposing to include similar language in § 226.8(j) for Covered Cyber Incident Reports and § 226.11(a)(4) for Supplemental Reports.

CIRCIA exempts any action required to carry out the reporting requirements in 6 U.S.C. 681b(a)(1)–(3) from compliance with PRA requirements codified in 44 U.S.C. 3506(c), 3507, 3508, and 3509. 6 U.S.C. 681b(f). This exemption includes actions taken by CISA to make changes to the questions included in the CIRCIA web-based Incident Reporting Form as described above and to solicit for optional information and data as part of CIRCIA reports.

4. Supplemental Report Specific Content

While CIRCIA includes some specific categories of content that a covered entity must include in a Covered Cyber Incident Report or Ransom Payment Report, CIRCIA does not contain any similar requirements regarding what content must be included in a Supplemental Report. Given that the purpose of a Supplemental Report is to provide CISA with additional or updated information regarding a previously reported covered cyber incident, the content required in a Supplemental Report generally will be a subset of the content required to be reported and optional content in a Covered Cyber Incident Report and/or Ransom Payment Report, tailored to the reason for the submission of the Supplemental Report and the information previously provided by the covered entity in the previously submitted CIRCIA Report.

A unique content request proposed to be contained in a Supplemental Report is information on the purpose for filing the Supplemental Report. CISA envisions providing a list of possible answers for this question, which may include (a) providing CISA with newly discovered information that makes a previously submitted Covered Cyber Incident Report or Supplemental Report more complete, (b) providing CISA with information that corrects or amends a

previously submitted Covered Cyber Incident Report or Supplemental Report, (c) informing CISA that the covered entity has made a Ransom Payment related to a previously reported covered cyber incident, or (d) informing CISA that the covered entity considers a previously reported covered cyber incident concluded and fully mitigated and resolved. CISA is also proposing to require that a Supplemental Report include the case identification number provided by CISA for the covered cyber incident with which the Supplemental Report is associated. This will facilitate pre-population of the Supplemental Report form and help CISA ensure that the Supplemental Report is properly assigned and maintained.

For Supplemental Reports being submitted by a covered entity for the purposes of informing CISA that the covered entity considers a previously reported covered cyber incident concluded and fully mitigated and resolved, CISA proposes including optional questions in the form that would allow a covered entity to provide information on the actual recovery date and time, and an estimate of the costs incurred to fully mitigate the incident, as well as any other financial losses (e.g., losses in productivity; losses in revenue) incurred due to the incident. This data would help inform assessments of the risks associated with and impacts of cyber incidents and will assist CISA in meeting some of the briefing and reporting requirements assigned to CISA under CIRCIA.

A small number of commenters requested a mechanism for a covered entity to “de-escalate” an incident (i.e., inform CISA when the covered entity discovers additional information that causes the entity to believe an incident for which it had previously submitted a Covered Cyber Incident Report does not actually meet the criteria for a covered cyber incident). CISA believes this scenario is simply one variation that a Supplemental Report may take and proposes to include questions tailored to this within the Supplemental Report portion of the user interface for occasions where a covered entity is using a Supplemental Report for this purpose. CIRCIA exempts any action required to carry out the reporting requirements in 6 U.S.C. 681b, including 6 U.S.C. 681b(a)(1)–(3), from compliance with PRA requirements codified in 44 U.S.C. 3506(c), 3507, 3508, and 3509. 6 U.S.C. 681b(f). This exemption includes actions taken by CISA to make changes to the questions included in the CIRCIA web-based Incident Reporting Form as described

above and to solicit for optional information and data as part of CIRCIA Reports.

5. Content in the DHS-Developed Model Reporting Form Not Included in Proposed CIRCIA Reporting Forms

As noted earlier, as part of its efforts to promote harmonization of Federal cyber incident reporting regulations and minimize the burden on entities that may need to comply with more than one cyber incident reporting requirement, DHS, informed by conversations with the CIRC, developed a Model Reporting Form. In support of harmonization of Federal cyber incident reporting requirements, CISA carefully considered the Model Reporting Form during the development of the proposed CIRCIA reporting form and strove to align the content required by the two forms where possible while still meeting the requirements, needs, and limitations imposed by CIRCIA. Consequently, the majority of the content that CISA is proposing be submitted via its reporting form is also requested in the Model Reporting Form and vice versa (*i.e.*, the majority of the content requested by the Model Reporting Form is proposed for inclusion in the CIRCIA reporting forms).

CISA ultimately determined that a small number of items contained in the Model Reporting Form were not appropriate for inclusion in the CIRCIA reporting forms or were only appropriate for inclusion on an optional basis. First, the Model Reporting Form includes a section where a reporting entity is afforded the opportunity to indicate if it believes one or more FOIA exemptions should apply to the information being submitted. CIRCIA Reports are statutorily exempt from disclosure under FOIA and any similar State, Local, and Tribal freedom of information laws, open government laws, sunshine laws, or similar laws requiring disclosure of information or records. 6 U.S.C. 681e(b)(2). Accordingly, the CIRCIA reporting form does not contain a similar section on FOIA exemptions that may apply under other authorities; however, it will contain a statement acknowledging this protection from disclosure under FOIA or similar laws pursuant to CIRCIA.

Second, the Model Reporting Form includes a number of questions related to whom the reporting entity has notified about the incident. This includes questions regarding whether the reporting entity has notified any governmental entities (*e.g.*, regulators or other departments or agencies, law enforcement, Congress) and, in the case of consumer data breaches or privacy

breaches, if the reporting entity has notified impacted individuals and provided them with guidance on how to take steps to protect themselves during an ongoing incident. CISA is proposing to include as required content in CIRCIA Reports information on a covered entity's notification or other form of engagement with law enforcement agencies. CISA, however, is not proposing to require that covered entities report whether they have notified other stakeholders, such as non-law enforcement government entities, Congress, or individuals potentially impacted by the incident. While some of these additional notifications may be of general interest to CISA and support more effective or efficient information sharing among partners, none are required for CISA to meet its obligations under CIRCIA. Accordingly, CISA is not proposing requiring that covered entities report any of this information in a CIRCIA Report. CISA may include optional questions on some of these topics so that covered entities who are interested in voluntarily providing this information to CISA may do so.

iv. Timing of Submission of CIRCIA Reports

1. Timing for Submission of Covered Cyber Incident Reports

Under 6 U.S.C. 681b(a)(1)(A), a covered entity that experiences a covered cyber incident must submit a Covered Cyber Incident Report to CISA "not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred." CISA has included proposed language in the regulation establishing this timeframe in § 226.5(a).

CISA acknowledges that the point at which a covered entity should have "reasonably believed" a covered cyber incident occurred is subjective and will depend on the specific factual circumstances related to the particular incident. Accordingly, CISA is not proposing a specific definition for the term "reasonably believes," nor is CISA attempting to prescribe a specific point in the incident life cycle at which a "reasonable belief" will always be realized. Rather, CISA is providing the following guidance to help covered entities understand when a "reasonable belief" generally is expected to have occurred.

CISA does not expect a covered entity to have reached a "reasonable belief" that a covered cyber incident occurred immediately upon occurrence of the incident, although this certainly may be true in some cases (*e.g.*, an entity receives a ransom demand

simultaneously with discovery that it has been locked out of its system). Oftentimes, an entity may need to perform some preliminary analysis before coming to a "reasonable belief" that a covered cyber incident occurred. This preliminary analysis may be necessary, for instance, to quickly rule out certain potential benign causes of the incident or determine the extent of the incident's impact. CISA believes that in most cases, this preliminary analysis should be relatively short in duration (*i.e.*, hours, not days) before a "reasonable belief" can be obtained, and generally would occur at the subject matter expert level and not the executive officer level. As time is of the essence, CISA expects a covered entity to engage in any such preliminary analysis as soon as reasonably practicable after becoming aware of an incident and is proposing including such a requirement in the regulatory text.

A number of stakeholders submitted comments in response to the RFI suggesting that a "reasonable belief" occurs when an entity has confirmed, determined, or otherwise definitively established that an incident was a covered cyber incident. CISA does not agree with those commenters, and instead interprets "reasonable belief" to be a much lower threshold than "confirmation." CISA additionally believes that if Congress had intended the timeframe for reporting to begin at confirmation of an incident, it would have used specific language making that clear. CISA believes few, if any, circumstances will occur where an extended investigation must be undertaken and concluded before an entity can form a "reasonable belief" that a covered cyber incident occurred.

2. Timing for Submission of Ransom Payment Reports

Under 6 U.S.C. 681b(a)(2)(A), a covered entity that makes a ransom payment must submit a Ransom Payment Report to CISA "not later than 24 hours after the ransom payment has been made." CISA has included proposed language in the regulation reflecting this timeframe in § 226.5(b).

Different regulations have taken different approaches to when a payment is considered to have been "made" by a party. Some regulations interpret a payment to have been made on the date the payment is disbursed (*e.g.*, sent, transmitted, submitted).³⁶⁴ Others

³⁶⁴ *Federal Acquisition Regulations*, 48 CFR 52.232-25 ("The Government considers payment as being made on the day a check is dated or the date

interpret a payment to have been made on the date the payment is received by the payee or otherwise becomes available to the payee.³⁶⁵ For some regulations, when the payment is made varies based on the method of payment.³⁶⁶

For purposes of this provision of the regulation, CISA proposes interpreting payment to have been made upon disbursement of the payment by the covered entity or a third party directly authorized to make a payment on the covered entity's behalf. CISA is proposing this approach for two main reasons. First, when disbursement of a payment was made is easier for a covered entity to determine than when a payment has cleared, settled, posted, or otherwise been made available to the payee. Selecting payment disbursement instead of payment settlement or clearance as the trigger for when the reporting timeline begins provides greater clarity and prevents a covered entity from having to try to determine when a payment has actually been received by or otherwise made available to the payee. Second, as discussed earlier in Section III.C.ii in this document, it is imperative that CISA receive reports of covered cyber incidents and ransom payments in a timely manner so CISA can more quickly identify adversary trends, TTPs, and vulnerabilities being exploited to be able to provide other entities early warnings and mitigation strategies to help them avoid becoming victims to similar attacks. By interpreting when a payment is made to be at the earlier point of payment disbursement, rather than the later point of payment receipt, posting, or settlement, CISA will be able to receive reports of ransom payments earlier and be better situated to achieve some of the ultimate goals that Congress authorized the regulation to achieve.

CISA recognizes that in certain situations, more than one third party may be involved in the disbursement of

of an electronic funds transfer.”); *IRS Tax Regulations*, 26 CFR 301.7502-1 (“[I]f the requirements of that section are met, a document or payment is deemed to be filed or paid on the date of the postmark stamped on the envelope or other appropriate wrapper (envelope) in which the document or payment was mailed.”).

³⁶⁵ *IRS Employment Tax Regulations*, 26 CFR 31.3406(a)-4 (“Amounts are considered paid when they are credited to the account of, or made available to, the payee. Amounts are not considered paid solely because they are posted (e.g., an informational notation on the payee’s passbook) if they are not actually credited to the payee’s account or made available to the payee.”).

³⁶⁶ *Prompt Payment Act Regulations*, 5 CFR 1315.4(h) (“Payment will be considered to be made on the settlement date for an electronic funds transfer payment or the date of the check for a check payment.”).

a ransom payment. For instance, a covered entity might send funds to an intermediate third party, who might then transmit the funds to a financial institution, who then transfers the payment to the account specified by the party demanding the ransom payment. In interpreting this regulatory provision, the reporting timeline shall be deemed to be initiated at the earliest instance of disbursement. Thus, in the example provided, disbursement has occurred and the timeline for reporting would be triggered when the covered entity sent funds to the intermediate third party. In a case where a covered entity authorizes an intermediate third party to transmit funds on its behalf to make a ransom payment but does not actually disburse funds itself at that time, the reporting timeline shall be deemed to be initiated when the intermediate third party disburses funds.

3. Timing for Submission of Supplemental Reports

Under 6 U.S.C. 681b(a)(3), a covered entity that has previously submitted a Covered Cyber Incident Report must “promptly” submit to CISA an update or supplement to that report if either: (a) “substantial new or different information becomes available”; or (b) “the covered entity makes a ransom payment after submitting a covered cyber incident report.” A covered entity is subject to these supplemental reporting obligations unless and until the covered entity notifies CISA that the incident that is the subject of the original Covered Cyber Incident Report “has concluded and has been fully mitigated and resolved.” Section 226.5(d) of the proposed regulation contains these Supplemental Reporting requirements.

a. Meaning of “Promptly”

CISA is proposing to use the statutory language contained in 6 U.S.C. 681b(a)(3) verbatim in the regulation to identify the timeframe and associated trigger for providing Supplemental Reports to CISA. As opposed to the statutory language for Covered Cyber Incident Reports and Ransom Payment Reports that contain specific numerical timeframes, CIRCIA requires Supplemental Reports to be submitted “promptly” upon the occurrence of either of the two identified triggering events. CISA interprets “promptly” to generally mean what it means colloquially, *i.e.*, without delay or as soon as possible.

CISA notes that one of the two potential triggering events for a Supplemental Report has a separate timeframe for reporting mandated in

CIRCIA. Specifically, making a ransom payment following the submission of a Covered Cyber Incident Report triggers a requirement for the covered entity to submit a Supplemental Report. See 6 U.S.C. 681b(a)(3). Given that CIRCIA requires covered entities to submit Ransom Payment Reports within 24 hours of making the ransom payment, CISA believes it is appropriate to interpret “promptly” to mean no longer than 24 hours after disbursement of the payment. Any other interpretation would result in a logical inconsistency where a covered entity would be able to extend the timeframe for reporting a ransom payment by filing a separate Covered Cyber Incident Report prior to making the ransom payment.

b. Meaning of “Substantial New or Different Information”

CISA proposes interpreting “substantial new or different information” as meaning information that (1) is responsive to a required data field in a Covered Cyber Incident Report that the covered entity was unable to substantively answer at the time of submission of that report or any Supplemental Report related to that incident, or (2) shows that a previously submitted Covered Cyber Incident Report or Supplemental Report is materially incorrect or incomplete in some manner. Together, these two provisions will help ensure that a covered entity has provided to CISA all required information related to a covered cyber incident in a timely fashion and that any material inaccuracies in a previously submitted Covered Cyber Incident Report or Supplemental Report are promptly corrected.

The first prong of the interpretation—information that is responsive to a required data field in a Covered Cyber Incident Report that the covered entity was unable to substantively answer at the time of submission of that report or any Supplemental Report related to that incident—is focused on filling informational gaps from prior reporting. For instance, if an entity stated in its Covered Cyber Incident Report that the vulnerability exploited in perpetrating the incident was “unknown at this time,” discovery of the exploited vulnerability would be information that meets this prong and would need to be reported promptly in a Supplemental Report. This prong is focused solely on completion of required data fields for which a covered entity previously did not have responsive or complete information at the time of filing a Covered Cyber Incident Report. CISA considers newly discovered information

for any previously unaddressed required data field to be substantial and to meet the meaning of “substantial new or different information.” If a covered entity discovers new information related to a question it has previously responded to, that information should be evaluated under the second prong, and would only be considered “substantial new or different information” that must be reported if it meets a materiality threshold.

The second prong of the interpretation—information that shows that a previously submitted Covered Cyber Incident Report or Supplemental Report is materially incorrect or incomplete in some manner—is focused on amendments or additions to content previously provided by a covered entity about a covered cyber incident. To reduce the burden of supplemental reporting on covered entities, CISA is proposing to limit supplemental reporting requirements under this prong to times when the amendment or addition would result in a material change in CISA’s understanding of the covered cyber incident. Limiting this prong to material changes will help ensure that CISA gets material updates in a timely manner while avoiding making a covered entity submit a Supplemental Report every time it learns anything new about the incident.

Examples of the types of information that CISA believes typically should be considered material include updated or corrected information on the TTPs used to perpetrate the incident; the discovery or identification of additional indicators of compromise; additional or corrected information related to the identity of the individual or individuals who perpetrated the incident; or identification of significant new consequences. Changes to the covered entity’s point of contact information should also be considered material and reported promptly. Additionally, while newly discovered information that is responsive to an “optional” question need not be reported, material corrections to previously submitted information must be reported even if the originally submitted information was submitted in response to an “optional” question.

Examples that generally would not be considered material include minor technical corrections or changes to the extent, but not the type, of the impact (unless the changes to the extent of the impact were orders of magnitude higher than what was previously reported). CISA encourages covered entities to provide that information to CISA, but covered entities are not required to do so. Similarly, CISA encourages covered

entities to voluntarily provide additional information that is not required by CIRCIA Reports but “enhances the situational awareness of cyber threats” consistent with 6 U.S.C. 681c(b).

While covered entities are not expected to submit Supplemental Reports for Ransom Payment Reports (unless the Ransom Payment Report is associated with a Covered Cyber Incident Report), CISA expects a covered entity to correct material inaccuracies. For example, if a covered entity submitted the incorrect phone number for its point of contact, the covered entity should correct its Ransom Payment report submission.

c. Meaning of “Concluded” and “Fully Mitigated and Resolved”

A covered entity’s supplemental reporting requirements remain in effect until the covered entity notifies CISA “that the covered cyber incident at issue has concluded and has been fully mitigated and resolved.” 6 U.S.C. 681b(a)(3). Although the point at which an incident is concluded and fully mitigated and resolved may vary based on the specific facts of the incident, reaching the following milestones is a good indication that an incident has been concluded and fully mitigated and resolved: (1) the entity has completed an investigation of the incident, gathered all necessary information, and documented all relevant aspects of the incident; and (2) the entity has completed steps required to address the root cause of the incident (*e.g.*, completed any necessary containment and eradication actions; identified and mitigated all exploited vulnerabilities; removed any unauthorized access). The completion of a lessons learned analysis (*i.e.*, after action report) is a valuable part of incident response, but CISA does not believe that such analysis needs to be completed for an incident to be considered concluded and fully mitigated and resolved. Similarly, CISA does not believe that all damage caused by the incident must have been fully addressed and remediated for an incident to be considered concluded and fully mitigated and resolved.

For an incident to be concluded and fully mitigated and resolved, a covered entity should have a good-faith belief that further investigation would not uncover any substantial new or different information about the covered cyber incident. If, following the provision of a notification to CISA that the covered entity believes the covered cyber incident to be concluded and fully mitigated and resolved, the covered entity becomes aware of any substantial

new or different information, the covered entity is responsible for submitting a Supplemental Report. In such a situation, CISA will consider the prior notification that the incident is concluded and fully mitigated and resolved to be rendered void and the covered cyber incident ongoing and active. The covered entity remains responsible for submitting Supplemental Information until such time as the covered cyber incident is concluded and fully mitigated and resolved and no new or different information indicates that the covered cyber incident is ongoing.

v. Report Submission Procedures

1. Submission of CIRCIA Reports to CISA

As discussed above, CISA is proposing that covered entities or third parties submitting CIRCIA Reports on behalf of a covered entity are required to do so using the web-based user interface or other mechanism subsequently approved by the Director. To submit a report using the web-based user interface, the submitter will need to have completed all required fields, to include, in the case of a third-party submitter, an attestation that the third party has been expressly authorized by the covered entity to submit the report on the covered entity’s behalf. In recognition that a covered entity may not have all the required information within the 72-hour time limit for submission of a Covered Cyber Incident Report, CISA may accept submission of a report where the response to some required answers is “unknown at this time,” “pending the results of additional investigation,” or some other similar option to submit the initial report.

CISA is proposing that, upon receipt of a report, CISA issue the covered entity (and, in the cases of a third-party submitter, the third party) a confirmation of receipt along with a unique case management number. The confirmation of receipt is simply meant to inform the covered entity that the report has been properly submitted to and received by CISA; the confirmation is not, however, an indication that a covered entity has necessarily met all of its reporting requirements. The case identification number is meant to facilitate tracking and performance of future actions related to the specific incident or ransom payment, to include supporting pre-population of data fields during the preparation of Supplemental Reports.

CISA intends to provide covered entities the opportunity to register with

CISA under this proposed rule. Registration would allow a covered entity to pre-populate a number of the required data fields, such as entity identifying information, on the proposed web-based CIRCIA Incident Reporting Form. Registering with CISA would allow a covered entity to submit certain information to CISA for use in future CIRCIA reporting. Any covered entity that had previously submitted a CIRCIA Report would also have the information they submitted stored for future use. CISA believes that allowing this optional registration, which is completely voluntary, would reduce the time burden associated with submitting a CIRCIA Report when required due to the advanced submission and pre-population of certain information that is required in a CIRCIA Report.

2. Process for Notifying CISA That an Incident Has Concluded and Been Fully Mitigated and Resolved

Covered entities have the option of notifying CISA that a previously reported covered cyber incident has concluded and has been fully mitigated and resolved. See 6 U.S.C. 681b(a)(3). Although notifying CISA that a previously reported covered cyber incident has concluded and been fully mitigated and resolved is not required, doing so terminates the covered entity's responsibility to provide Supplemental Reports.³⁶⁷

CISA is proposing that the process for notifying CISA that a previously reported covered cyber incident has concluded and been fully mitigated and resolved is through the submission of a Supplemental Report. A covered entity or a third party submitting a notification on a covered entity's behalf simply would indicate in the Supplemental Report that the purpose (or one of the purposes) of the Supplemental Report is to notify CISA that the covered entity believes the incident has concluded and been fully mitigated and resolved. The process for doing so would be the same as for the submission of any other Supplemental Report, which is described in § 226.6 of the regulation, although the submitter may be asked certain questions related to how the incident was concluded, mitigated, and resolved.

³⁶⁷ As noted in Section IV.D.iv.3.c, CISA interprets notification to terminate the requirement to submit Supplemental Reports only if no substantial new or different information is subsequently discovered by the covered entity. CISA believes the discovery of such information would indicate that the covered entity's belief that the incident was concluded, fully mitigated, and resolved, was inaccurate, rendering the declaration of closure void.

3. Third-Party Submission of CIRCIA Reports

CIRCIA authorizes covered entities to use third parties to submit Covered Cyber Incident Reports or Ransom Payment Reports on behalf of the covered entity. Specifically, 6 U.S.C. 681b(d)(1) states "[a] covered entity that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit the required report under subsection (a)." The following subsections address various aspects of third-party submission of CIRCIA Reports.

a. Who May Serve as a Third-Party Submitter

In response to the RFI, a number of commenters requested that CISA clarify the types of third parties authorized to submit CIRCIA Reports on behalf of a covered entity. A few commenters encouraged CISA to allow anyone approved by a covered entity to be able to submit a report on their behalf, while others encouraged CISA take the opposite approach and limit the types of entities that could serve as a third-party submitter. Some commenters provided specific types of entities that they believe CISA should authorize to serve as third-party submitters, including, but not limited to, ISACs, incident management firms, external legal representatives, state water associations, and SLTT jurisdictions to whom an entity is also obligated to report.

In 6 U.S.C. 681b(d)(1), Congress provides a list of entities that covered entities might use to report Covered Cyber Incident Reports or Ransom Payment Reports on the covered entity's behalf. Specifically, 6 U.S.C. 681b(d)(1) states a covered entity that is required to submit a Covered Cyber Incident Report or a Ransom Payment Report "may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm," to submit the required report. As Congress preceded this list with the phrase "such as," CISA interprets the list to be illustrative examples and not a closed list of which categories of third parties a covered entity may use to submit CIRCIA Reports on its behalf.

The few comments CISA received on this topic demonstrate that there may be a wide variety of types of organizations or individuals that a covered entity may wish to have submit a report on the covered entity's behalf. CISA does not at

this time see any policy rationales for limiting the types of organizations or individuals that a covered entity can choose to submit a report on the covered entity's behalf, especially considering that the responsibility for complying with the regulation remains with the covered entity even if it uses a third party to submit a report on its behalf. 6 U.S.C. 681b(d)(3). On the contrary, CISA sees value in allowing the covered entity the flexibility to determine which party is best situated to submit CIRCIA Reports on its behalf. Accordingly, CISA is proposing that a covered entity may use any organization or individual it chooses to submit a CIRCIA Report on its behalf.

While CISA is proposing that a covered entity may select any organization or individual it chooses to submit a report on its behalf, the third party must be expressly authorized by the covered entity to submit a report on the covered entity's behalf for the report to be accepted by CISA for purposes of compliance with the regulation. As the requirement to submit a timely and accurate report under CIRCIA remains in all cases with the covered entity itself, it is imperative that the covered entity have expressly authorized a third party to submit a report on its behalf. Express authorization can be granted in any number of ways, including verbally or in writing. Any report submitted by a third party that has not been expressly authorized by the covered entity to submit the report will not be imputed to the covered entity or considered by CISA for purposes of CIRCIA compliance.³⁶⁸

To better ensure that a report being submitted by a third party is being submitted subject to the express authorization of the covered entity, CISA is proposing requiring the third party to include in the submission an attestation that it has been expressly

³⁶⁸ Historically, CISA has on occasion received reports from individuals or organizations not directly affiliated with the entity experiencing the impact or otherwise not authorized to report the incident on behalf of the affected entity. This may occur, for instance, where an individual or organization is directly experiencing an incident that is causing cascading effects on another entity's information systems, where an individual or organization has become aware of what it believes to be an incident on another entity's cyber system, or where an employee of an organization that is experiencing a cyber incident elects to report an incident despite not having authority from the entity to report on its behalf. In these and other situations where an individual wants to submit a report about an incident without the consent of the covered entity experiencing the incident, it may do so through CISA's voluntary reporting portal; however, the information contained in that report will not be imputed to the entity experiencing the incident, nor will it be considered a report submitted for the purposes of CIRCIA compliance.

authorized by the covered entity to submit the report. This likely would be accomplished by requiring a third party to check a box in the online form attesting to this, or some other similar electronic mechanism. As a general legal prohibition against knowingly providing false information to the Federal government exists (see 18 U.S.C. 1001), CISA believes that requiring this attestation from the third party is a sufficient deterrent to prevent individuals or organizations from seeking to submit a CIRCIA Report on behalf of a covered entity without express authorization.

CISA considered requiring a third party to provide some sort of evidence verifying its claim of authorization, such as a contract or email clearly conferring the authority. CISA believes, however, that the deterrent value of requiring the third party to attest in the reporting form that they have the express authority to submit on behalf of the covered entity is sufficient to prevent most cases of unauthorized submissions, and that the marginal benefit provided by requiring evidence of such express authorization is exceeded by the burden of providing specific evidence. Additionally, CISA believes requiring evidence beyond an attestation has the potential to disincentivize the use of third-party submitters, which CISA believes may be detrimental to organizations seeking to leverage third parties to assist with incident response and recovery.

Some commenters suggested that a third party must be in a formal, contractual relationship with the covered entity to submit on the entity's behalf. CISA believes this level of formality is not necessary and may not be practical in certain arrangements, such as where an entity is using an ISAC or an SLTT Government entity to submit on the entity's behalf. Accordingly, CISA is not proposing that a covered entity and third party must have entered into a formal, contractual agreement for the third party to be authorized to submit on the covered entity's behalf.

b. Types of CIRCIA Reports a Third Party May Submit

Section 681b(d)(1) of title 6, United States Code, states “[a] covered entity that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, Information Sharing and Analysis Organization, or law firm, to submit the required report under subsection (a).” The subsection that clause refers to is 6

U.S.C. 681b(a) which, among other things, sets forth the general requirements related to Covered Cyber Incident Reports, Ransom Payment Reports, and Supplemental Reports. Although the first part of 6 U.S.C. 681b(d)(1) only mentions Covered Cyber Incident Reports and Ransom Payment Reports, CISA interprets the phrase “submit the required report under subsection (a)” to cover not only Covered Cyber Incident Reports and Ransom Payment Reports, but Supplemental Reports as well.

CISA is not aware of any persuasive policy reasons for allowing a covered entity to use a third party to submit a Covered Cyber Incident Report or Ransom Payment Report on the entity's behalf, but not allow a third party to submit a Supplemental Report to CISA on the covered entity's behalf; nor does CISA believe that was Congress's intent. Conversely, CISA believes that there would be benefits to allowing a covered entity to use a third party to submit a Supplemental Report on the covered entity's behalf, especially in cases where a covered entity used the same third party to submit a previous report on the covered entity's behalf. Accordingly, CISA is proposing that covered entities be allowed to use a third party to submit and update any type of CIRCIA Report—*i.e.*, a Covered Cyber Incident Report, Ransom Payment Report, Joint Covered Cyber Incident and Ransom Payment Report, or Supplemental Report—on behalf of the covered entity, so long as any other regulatory requirements related to using a third party to submit a CIRCIA Report on a covered entity's behalf are met. CISA further proposes that a covered entity need not have used a third party to submit its initial report (be it a Covered Cyber Incident Report or a Ransom Payment Report) to use a third party to submit a Supplemental Report or vice versa. Similarly, a covered entity can use different third-party submitters for subsequent CIRCIA Reports. Whether a covered entity submits a report itself or uses a third party, and who the third-party submitter is if one is used, is something the covered entity may decide each time it submits a CIRCIA Report.

CISA also is proposing to allow third parties to submit a single report on behalf of multiple covered entities if the circumstances leading to the reporting requirement for the various covered entities is similar enough to be reported collectively. For example, if a single cyber incident perpetrated against a CSP, managed service provider, or other third-party service provider impacts a number of the service provider's customers in a similar fashion, and

those impacted customers are covered entities, the service provider may be well situated to submit a single report on behalf of itself and some or all of its affected customers. In such a situation, the rules regarding third party submissions still would apply, with the third-party service provider needing to have the authorization to report on behalf of any customer on whose behalf it is reporting, as well as the ability to provide all of the information that the covered entity customer would have had to submit on its own, were it submitting its own CIRCIA Report. CISA believes this proposed approach will help reduce reporting burden while still providing a complete picture of the covered cyber incident.

c. Process for Submission of CIRCIA Reports by Third Parties

CISA is proposing that the process for the submission of a report by a third party on behalf of the covered entity be the same process as that which exists for the submission of a report by the covered entity itself, with two minor modifications. First, as noted in Section IV.E.iii.1.d in this document, CISA is proposing that a third-party submitter must attest in the reporting form to the fact that it has been authorized by the covered entity to submit the report on behalf of the covered entity. Second, as noted in Section IV.E.iii.4 in this document, CISA is proposing that any CIRCIA Report submitted by a third party include a small number of additional questions to ensure that CISA has a name and point of contact information for both the third-party submitter and the covered entity on whose behalf the report is being submitted. CISA's rationale for these two minor modifications are discussed in the respective sections of this document cited earlier in this paragraph.

d. Burden of Compliance When a Covered Entity Uses a Third Party To Submit a Report

A number of comments received by CISA in response to the RFI encourage CISA to confirm that the responsibilities for complying with the CIRCIA regulatory requirements do not shift from the covered entity to a third party when the covered entity uses a third party to submit a CIRCIA Report on the covered entity's behalf. CISA interprets the statutory language to affirm that use of a third party does not shift compliance responsibilities from the covered entity to the third party. While the statute authorizes a covered entity to use a third party to submit a report on the covered entity's behalf, it does not

at any point authorize CISA to hold a third-party submitter accountable for a covered entity's reporting responsibilities, nor does it at any point absolve the covered entity of its reporting obligations. In fact, 6 U.S.C. 681b(d)(3) indicates the contrary, stating third-party reporting "does not relieve a covered entity from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission." While 6 U.S.C. 681b(d)(3) does not mention Supplemental Reports, there similarly is nothing in the statute absolving a covered entity of the responsibility for submitting Supplemental Reports as required or shifting that responsibility to a third party, and CISA is unaware of any policy rationales for treating Supplemental Reports differently in this circumstance from Covered Cyber Incident Reports or Ransom Payment Reports.

Additional support for the interpretation that the burden does not shift to the third party when a covered entity uses a third party to submit on its behalf is found in 6 U.S.C. 681d(a), which explicitly refers to covered entities as the entity to which CISA is authorized to issue an RFI or a subpoena when it believes a covered entity has failed to submit a required CIRCIA Report. Likewise, the venue provision contained in 6 U.S.C. 681d(c)(2)(B) focuses on where the covered entity resides, is found, or does business for purposes of determining where a civil action may be brought. These sections make clear that any enforcement action for noncompliance is to be brought against the covered entity, not a third party that submitted (or failed to submit) a report on the covered entity's behalf. Consistent with this understanding, CISA interprets it to be the covered entity's responsibility to ensure that any CIRCIA Report submitted by a third-party on the covered entity's behalf is accurate and to correct any inaccurate or update incomplete information through the submission of a Supplemental Report.

e. Third Party Ransom Payments and Duty To Advise

Pursuant to 6 U.S.C. 681b(d)(2), a third party that makes a ransom payment on behalf of a covered entity impacted by a ransomware attack is not required to submit a Ransom Payment Report on behalf of itself for such ransom payment. The obligation to report that ransom payment remains with the covered entity, although the covered entity may authorize the third party who made the ransom payment, or a different third party, to submit a

Ransom Payment Report to CISA on the covered entity's behalf. Accordingly, CISA proposes reflecting this in the proposed regulation by stating in § 226.12(d) that a third party that makes a ransom payment on behalf of a covered entity impacted by a ransomware attack is not required to submit a Ransom Payment Report on behalf of itself for the ransom payment.

Pursuant to 6 U.S.C. 681b(d)(4), however, a third party that knowingly makes a ransom payment on behalf of a covered entity impacted by a ransomware attack does have a duty to advise that covered entity of its obligation to report the ransom payment to CISA. CISA proposes codifying this in the regulation in § 226.12(d). CISA recognizes that there may be situations where a chain of third parties is involved in making a ransom payment on behalf of a covered entity. CISA intends the duty to advise the covered entity of its reporting obligations to apply only to a third party who is directly engaging with the covered entity knowingly for the purposes of making the ransom payment. Third parties involved in the payment of the ransom who do not have a direct relationship with the covered entity or who are not aware that the funds being transmitted are for the purpose of paying a ransom payment are not obliged to inform the covered entity of CIRCIA reporting requirements.

vi. Request for Comments on Proposed Manner, Form, and Content of Reports

CISA seeks comments on all aspects of the proposed manner, form, and content of CIRCIA Reports, and the proposed procedures for submitting CIRCIA Reports, to include the following:

52. The proposed use of a web-based form as the primary means of submission of CIRCIA Reports, the proposed maintenance of telephonic reporting as a back-up reporting option, assumptions used in evaluating different possible manners of submission, and the possibility of allowing automated (*i.e.*, machine-to-machine) reporting or other manners of submission in the future at the discretion of the Director.

53. The proposal to use a single, dynamic, web-based form for the submission of all types of CIRCIA Reports, regardless of whether the report is submitted by a covered entity or a third party on the covered entity's behalf.

54. The content CISA is proposing be included in all CIRCIA Reports and the specific proposed content for Covered Cyber Incident Reports, Ransom

Payment Reports, Joint Covered Cyber Incident and Ransom Payment Reports, and Supplemental Reports, respectively, as well as additional content CISA is proposing to require when a third-party submitter is used to submit a CIRCIA Report on behalf of a covered entity.

55. The proposals CISA is making related to the timing of reports, including the proposed interpretation of "reasonable belief," the proposed interpretation for when a ransom payment "has been made," the proposed meaning of "promptly," the proposed meaning of "substantial new or different information," and the proposed meaning of "concluded" and "fully mitigated and resolved."

56. The proposed CIRCIA Report submission procedures, to include the process for notifying CISA that an incident has concluded and been fully mitigated and resolved.

57. The proposed rules regarding the submission of a report by a third party on behalf of a covered entity, to include who may serve as a third-party submitter, the types of CIRCIA Reports a third party may submit on behalf of a covered entity, the burden of compliance when a covered entity uses a third party to submit a report, and a third party's duty to advise a covered entity of the covered entity's CIRCIA reporting requirements when the third party makes a ransom payment on behalf of a covered entity.

F. Data and Records Preservation Requirements

Under CIRCIA, any covered entity that submits a CIRCIA Report must preserve data relevant to the reported covered cyber incident or ransom payment in accordance with procedures established in the final rule. 6 U.S.C. 681b(a)(4). To implement this requirement, CISA is to include in the final rule, a clear description of the types of data that covered entities must preserve, the period of time for which the data must be preserved, and allowable uses, processes, and procedures. See 6 U.S.C. 681b(c)(6).

As noted earlier, a covered entity's use of a third party to submit a CIRCIA Report on behalf of the covered entity does not shift compliance responsibilities from the covered entity to the third party. See IV.D.v.3.d. That principle holds true for data preservation requirements as well. A covered entity will retain responsibility for complying with the data preservation requirements established in the final rule even when the covered entity has a third party submit a required CIRCIA Report to CISA on behalf of the covered entity.

i. Types of Data That Must Be Preserved

The preservation of data and records³⁶⁹ in the aftermath of a covered cyber incident serves a number of critical purposes, such as supporting the ability of analysts and investigators to understand how a cyber incident was perpetrated and by whom. Access to forensic data, such as records and logs, can help analysts uncover how malicious cyber activity was conducted, what vulnerabilities were exploited, what tactics were used, and so on, which can be essential to preventing others from falling victim to similar incidents in the future. How an incident was perpetrated may not be immediately identifiable upon discovery, and the failure to properly preserve data or records during the period of initial incident response can render it difficult to subsequently perform this analysis. This can especially be true in incidents involving zero-day vulnerabilities or highly complex malicious cyber activity by nation state threat actors, such as the “SUNBURST” malware that compromised legitimate updates of customers using the SolarWinds Orion product or the Hafnium campaign on Exchange servers, with the full extent, cause, or attribution of an incident often not being known until months after the initial discovery.³⁷⁰

Preservation of data is also central to law enforcement’s ability to investigate and prosecute the crime. As stated by the Department of Justice (DOJ) in their guidance for Federal prosecutors entitled *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, “Electronic records such as computer network logs, email, word processing

files, and image files increasingly provide the government with important (and sometimes essential) evidence in criminal cases.”³⁷¹ Failure to properly preserve relevant data and other forensic evidence can make identification and prosecution of the perpetrators of a cyber incident significantly harder, if not impossible.

In order to support these activities, and consistent with the authorities provided to CISA in 6 U.S.C. 681b(a)(4) and 681(c)(6), CISA is proposing requiring covered entities to preserve a variety of data and records related to any covered cyber incidents or ransom payments reported to CISA in a CIRCIA Report. Specifically, CISA is proposing to require covered entities preserve data and records relating to communications between the covered entity and the threat actor; indicators of compromise; relevant log entries, memory captures, and forensic images; network information or traffic related to the cyber incident; the attack vector; system information that may help identify vulnerabilities that were exploited to perpetrate the incident; information on any exfiltrated data;³⁷² data and records related to any ransom payment made; and any forensic or other reports about the cyber incident produced or procured by the covered entity. See § 226.13(b).

CISA developed the proposed list of data and records to be preserved based upon its own experience with conducting incident detection, response, prevention, and analysis; by reviewing both best practices related to incident management, data preservation, and post-incident forensic analysis and stakeholder recommendations provided in response to the CIRCIA RFI and at the CIRCIA listening sessions; and following consultations with various Federal partners, to include the FBI and DOJ. Each of the proposed categories of data and records contains information directly relevant to questions and reporting elements of incident reports, as well as potentially helps CISA or other investigators identify and understand the TTPs used to perpetrate the incident, the vulnerabilities exploited in doing so, and potentially the identity of the perpetrator of the incident. The data and records proposed

for preservation additionally may be useful in subsequent law enforcement investigations and prosecution of the individual or individuals who perpetrated the incident.

A covered entity that has any of the data or records listed above must preserve those data or records regardless of what format they are in, whether they are electronic or not, located onsite or offsite, found in the network or in the cloud, etc. A covered entity is not, however, required to create any data or records it does not already have in its possession based on this regulatory requirement. The requirement for a covered entity to preserve data or records applies only to the extent the entity already has created, or would be creating them, irrespective of CIRCIA.

CISA is aware that retaining data and records is not without cost. In recognition of this, CISA attempted to reduce or focus the list of items to be retained to those that CISA believes would most likely be of value in support of future analysis or investigation. For instance, rather than require covered entities retain all log entries or memory captures from the time of the incident in case any of them may have contained pertinent data, CISA is proposing to limit this to log entries, memory captures, or forensic images that the covered entity believes in good faith are relevant to the incident. Similarly, CISA is not proposing that a covered entity be required to preserve copies of all data that was exfiltrated during an incident, but rather simply proposes that a covered entity preserve information sufficient to understand what type of and how much data was exfiltrated.

ii. Required Preservation Period

CISA is proposing that covered entities that submit CIRCIA Reports must begin preserving the required data at the earlier of either (a) the date upon which the entity establishes a reasonable belief that a covered cyber incident has occurred, or (b) the date upon which a ransom payment was disbursed, and must preserve the data for a period of no less than two years from the submission of the latest required CIRCIA Report submitted pursuant to § 226.3, to include any Supplemental Reports. Accordingly, if a covered entity only submits a single CIRCIA Report to CISA on a covered cyber incident or ransom payment, then the data preservation obligation is two years from the submission of the Covered Cyber Incident Report, Ransom Payment Report, or Joint Covered Cyber Incident and Ransom Payment Report. If, however, a covered entity submits one or more Supplemental Reports on a

³⁶⁹ The section in CIRCIA addressing this topic, 6 U.S.C. 681b(a)(4), uses the terms “data” and “information” at different times to characterize what a covered entity must preserve. CIRCIA does not, however, define either term. Rather than add to, or attempt to select from, the numerous definitions that have been proffered for both terms in a wide variety of cyber-related resources, CISA is proposing instead to include in the regulation a list of items that a covered entity will be required to preserve. See proposed § 226.13(b). The proposed list includes data and information in various forms, such as logs, images, registry entries, and reports. To better reflect the spectrum of information CISA is proposing to require entities to preserve, and in recognition of the fact that the term “records” is commonly used in the area of data or records retention, CISA is proposing to use the term “data and records” instead of simply “data” or “information.”

³⁷⁰ See, e.g., Adam J. Hart, *Evidence Preservation: The Key to Limiting the Scope of a Breach*, American Bar Association Cybersecurity and Data Privacy Committee Newsletter (Spring 2021), available at https://www.americanbar.org/groups/tort_trial_insurance_practice/committees/cyber-data-privacy/evidence-preservation/ (hereinafter “*Evidence Preservation*”).

³⁷¹ Department of Justice Computer Crime and Intellectual Property Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* at ix (2009), available at <https://www.justice.gov/criminal/criminal-ccips/ccips-documents-and-reports>.

³⁷² CISA is not proposing that a covered entity be required to preserve copies of all of the exfiltrated data; rather, CISA is proposing that a covered entity preserve information related to the data, such as the type and amount of data exfiltrated.

single covered cyber incident or ransom payment, the two-year retention period restarts at the time of submission of each Supplemental Report.

In establishing this proposed two-year timeframe, CISA considered existing best practices regarding preservation of information related to cyber incidents, data retention or preservation requirements from comparable regulatory programs, and comments received on this issue from stakeholders in response to the CIRCIA RFI and at CIRCIA listening sessions. In Section 3.4.3 of its *Computer Security Incident Handling Guide*,³⁷³ NIST discusses best practices for retaining evidence in the aftermath of a cybersecurity incident. Specifically, NIST Special Publication 800–61 Revision 2 (NIST SP 800–61r2) encourages organizations to establish policies regarding retention of evidence from an incident and states that “[m]ost organizations choose to retain all evidence for months or years after the incident ends.” In determining how long an entity should choose to preserve evidence, NIST recommends entities consider three factors. First, NIST notes that evidence may be needed in order to prosecute the threat actor which, in some cases, may take several years. On this point, NIST also notes that sometimes evidence that seems insignificant at the time of the incident will become more important in the future. The second factor NIST suggests entities consider is any existing internal data retention policies. As a point of reference, NIST notes that the General Records Schedule for Information Systems Security Records requires Federal departments and agencies to maintain computer security incident handling, reporting, and follow-up records for three years after all necessary follow-up actions have been completed.³⁷⁴ The final factor NIST mentions as something that should be considered is cost. NIST notes that certain items preserved as evidence generally may be inexpensive individually, but costs can be substantial if an organization stores such items for years. Outside of noting the three-year retention period included in the General Records Schedule, NIST SP 800–61r2 does not recommend a specific timeframe as a best practice for data preservation.

While most existing cyber incident reporting requirements do not include timeframes specifically targeted at

preservation of records related to a cyber incident, many do have broader recordkeeping requirements that frequently apply to cyber incident reports and/or other data or records related to a reportable cyber incident. For instance, facilities subject to CFATS are required to maintain records on incidents and breaches of security for three years.³⁷⁵ The NRC similarly requires regulated entities to maintain a copy of any written report submitted to the NRC on a cyber incident for three years.³⁷⁶ MTSA requires covered facilities to retain all records related to MTSA, including those related to cybersecurity incidents, for at least two years.³⁷⁷ And while not a regulation, M–21–31, “Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents,” requires Federal government entities subject to Executive Order 14028, “Improving the Nation’s Cybersecurity,” to retain most logs and certain other items related to cybersecurity incidents for a period of 30 months.³⁷⁸

CISA did not receive many comments from stakeholders on the topic of data preservation in response to the RFI or at CIRCIA listening sessions, but those stakeholders who did comment on the length of preservation generally recommended timeframes consistent with those identified above. Specifically, one commenter recommended requiring data be preserved for no longer than two years,³⁷⁹ one commenter recommended requiring data be preserved for no longer than three years,³⁸⁰ one commenter recommended being consistent with M–21–31,³⁸¹ and one commenter stated that data should be preserved for as long as needed, but not in perpetuity.³⁸² While not providing specific recommendations on the duration of preservation requirements, at least two commenters did note that data preservation can be costly, and encouraged CISA to develop

³⁷⁵ 6 CFR 27.255(a).

³⁷⁶ 10 CFR 73.77(d)(12).

³⁷⁷ 33 CFR 105.225(a).

³⁷⁸ See Office of Management and Budget, M–21–31, *Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (Aug. 27, 2021), available at <https://www.fedramp.gov/2023-07-14-fedramp-guidance-for-m-21-31-and-m-22-09/>.

³⁷⁹ Comments submitted by SAP, CISA–2022–0010–0114.

³⁸⁰ Comments submitted by the National Association of Chemical Distributors, CISA–2022–0010–0056.

³⁸¹ Comments submitted by Sophos, Inc., CISA–2022–0010–0047.

³⁸² Comments submitted by the American Chemistry Council, CISA–2022–0010–0098.

preservation requirements that are not overly burdensome and limited in scope and duration.³⁸³

Based on the above, CISA believes that a data preservation requirement typically lasting anywhere between two and three years would be consistent with existing best practices across industry and the Federal government, would be implementable by the regulated community, and would achieve the purposes for which data preservation is intended under CIRCIA. Recognizing that the costs for preserving data increase the longer the data must be retained, and wanting to limit costs of compliance with CIRCIA where possible without sacrificing the ability to achieve the purposes of the regulation, CISA thus is proposing that covered entities must preserve the required data and records for the lower end of the spectrum of best practice for data preservation, *i.e.*, a period of two years, unless substantial new or different information is discovered or additional actions occur that require the submission of a Supplemental Report and a commensurate extension of the data preservation timeframe.

iii. Data Preservation Procedural Requirements

Section 681b(c)(6) of title 6, United States Code, requires CISA to include in the final rule a clear description of the processes and procedures a covered entity must follow when preserving data. In light of the different manners in which the various required data and records can be stored, CISA is proposing to give covered entities significant flexibility in determining how to preserve the data and records, so long as the preservation method retains all salient details. This may include electronic or non-electronic (*i.e.*, hard copy) storage, onsite or offsite storage, network or cloud storage, and active or cold (*i.e.*, archived) storage. CISA believes that this flexibility will allow a covered entity to determine the most cost-effective way to preserve the data and records given the entity’s specific circumstances and the nature and format of the data and records being preserved.

CISA is proposing to impose two limitations on this flexibility, however. First, CISA is proposing that the covered entity must store the data and records in a manner that allows the data and records to be readily accessible and retrievable by the covered entity in

³⁸³ See, *e.g.*, Comments Submitted by CTIA, CISA–2022–0010–0070, and the Information Technology Industry Council, CISA–2022–0010–0097.

³⁷³ NIST SP 800–61r2, *supra* note 362, at 41.

³⁷⁴ National Archives, *General Records Schedule 3.2: Information Systems Security Records*, Item 020 (Jan. 2023), available at <https://www.archives.gov/records-mgmt/grs.html>.

response to a lawful government request. CISA does not intend for this provision to require entities to maintain the data onsite and have it immediately available upon request. Rather, CISA expects a covered entity to be able to retrieve and provide the data and records in response to a lawful government request within a reasonable amount of time.

Second, CISA is proposing to require covered entities to employ reasonable safeguards to protect the data and records against unauthorized access or disclosure, deterioration, deletion, destruction, and alteration. These safeguards must include protections against both natural and man-made, intentional and unintentional events, including cyber incidents. NIST Special Publication 1800–25, “Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events,” provides examples of the types of best practices that a covered entity might employ to meet this proposed requirement.

iv. Request for Comments on Proposed Data Preservation Requirements

CISA seeks comments on the proposed data preservation requirements, to include:

58. The types of data CISA is proposing covered entities preserve.

59. The proposed length of time covered entities must preserve data for.

60. The proposed procedural requirements governing the preservation of data.

61. Any other aspect of the proposed data preservation requirements.

G. Enforcement

i. Overview

CIRCIA provides a variety of mechanisms for CISA to use if CISA believes that a covered entity has failed to submit a CIRCIA Report in accordance with CIRCIA regulatory requirements. See 6 U.S.C. 681d. The potential approaches CISA has to address noncompliance include issuance of an RFI (6 U.S.C. 681d(b)), issuance of a subpoena (6 U.S.C. 681d(c)(1)), referral to the Attorney General to bring a civil action to enforce the subpoena and/or pursue a potential contempt of court (6 U.S.C. 681d(c)(2)), and other enforcement mechanisms to include potential acquisition penalties, suspension, and debarment (6 U.S.C. 681b(c)(8)(B)(ii)). Section 681b(c)(8)(B) of title 6, United States Code, requires CISA to include in the final rule procedures to carry out these enforcement provisions. Sections 226.14 through 226.17 of the proposed rule

contain CISA’s proposed procedures for each of these enforcement mechanisms, each of which is described in greater detail below.

Pursuant to 6 U.S.C. 681d(e), CISA must consider certain factors when determining whether to exercise any of these enforcement authorities. Specifically, CIRCIA mandates the Director take into consideration the complexity of determining whether a covered cyber incident occurred, and the covered entity’s prior interaction with CISA or its understanding of the policies and procedures for reporting for covered cyber incidents and ransom payments, as part of the process for evaluating whether to exercise an enforcement mechanism. CISA is proposing to include this statutory requirement essentially verbatim in § 226.14(b) of the proposed regulation. CISA will develop policies and procedures to ensure that the factors stated above are applied similarly to covered entities in similar circumstances.

CIRCIA additionally states that its enforcement provisions do not apply to SLTT Government Entities. 6 U.S.C. 681d(f). CISA proposes including this SLTT exclusion in § 226.14(a). What qualifies as a SLTT Government entity is defined in proposed § 226.1 and discussed in Section IV.A.iv.12 in this document.

ii. Request for Information

CIRCIA authorizes the Director to request information from a covered entity if the Director has reason to believe that the covered entity has experienced a covered cyber incident or made a ransom payment but failed to report the covered cyber incident or ransom payment in accordance with CIRCIA regulation. 6 U.S.C. 681d(b)(1). Through an RFI, the Director may request additional information from the covered entity to confirm whether or not a covered cyber incident or ransom payment occurred. 6 U.S.C. 681d(b)(1). Proposed § 226.14(c) contains the language CISA is proposing regarding CISA’s authority to issue an RFI, the form and content of an RFI, requirements a covered entity must follow to adequately respond to the RFI, the treatment of information included in a response to an RFI, and the inability for the issuance of an RFI to be appealed.

1. Issuance of Request

Proposed § 226.14(c) begins with a description of CISA’s authority to issue an RFI. The proposed language starts first with the acknowledgement that the Director has the authority to delegate

the issuance of an RFI, and then identifies the two different scenarios that may be the basis of the issuance of an RFI.

Although CIRCIA prohibits the delegation of the Director’s subpoena authority to another individual, CIRCIA does not similarly restrict who may issue an RFI. To provide CISA with additional flexibility regarding who may be able to issue an RFI, CISA is proposing to allow an RFI to be issued by either the Director or a designee of the Director. This would allow the Director to formally designate another individual (or more than one individual) as having the authority to issue an RFI. CISA believes this flexibility will help ensure CISA’s ability to issue RFIs in a timely manner, which may be essential in a rapidly unfolding, potentially substantial cyber incident. Accordingly, CISA proposes defining the Director in § 226.1 to include the Director of CISA or any designee.

Section 681d(b)(1) of title 6, United States Code, authorizes CISA to issue an RFI when CISA has reason to believe that a covered entity has experienced a covered cyber incident or made a ransom payment, but failed to report it “in accordance” with 6 U.S.C. 681b(a). CISA proposes including this authority in § 226.14(c)(1), which would authorize the issuance of an RFI to a covered entity when CISA has reason to believe that the entity experienced a covered cyber incident or made a ransom payment but failed to report the incident or payment in accordance with section 226.3. CISA interprets this language to allow CISA to issue an RFI in two distinct circumstances. First, CISA interprets this to allow CISA to issue an RFI when it believes a covered entity failed to report a covered cyber incident it experienced or a ransom payment it made. Second, CISA interprets this to allow issuance of an RFI to receive additional information following a covered entity’s submission of a report that CISA believes is deficient or otherwise noncompliant. This second scenario includes when CISA believes a covered entity failed to submit a Supplemental Report as required.

A plain reading of 6 U.S.C. 681d(b)(1) makes it clear that CISA is authorized to issue an RFI when CISA believes a covered entity experienced a covered cyber incident or ransom payment but failed to report it. That section of CIRCIA also provides additional context for what the Director, or Director’s designee, may use to determine that a covered entity failed to submit a required CIRCIA Report. Specifically,

CIR CIA states that CISA may base its decision to issue an RFI (or subpoena, if necessary) on public reporting or information in the possession of the Federal government. CISA proposes including this in § 226.14(c)(1) of the proposed regulation. CISA construes “information in the possession of the Federal government” broadly, to include, among other categories, information derived by CISA analysis, information reported by the covered entity, information from other sources typically used or shared by the government, or any combination of such information.

CISA interprets the language of 6 U.S.C. 681d(b)(1) to also authorize CISA to issue an RFI in cases where a covered entity submitted a report, but the report was deficient or otherwise noncompliant. For a number of reasons, CISA believes this to be the correct interpretation. First, CISA interprets the phrase “in accordance” to not only require that a covered entity submitted a report, but that it did so in a manner that complies with all the CIR CIA regulatory requirements for a report of the type in question. CISA believes that the use of the phrase “to confirm whether or not a covered cyber incident or ransom payment has occurred” in 6 U.S.C. 681d(b)(1) also supports this interpretation. CISA interprets “confirm” to include verification, thus allowing CISA to request information from a covered entity necessary for CISA to confirm (*i.e.*, verify) that an incident or payment discussed in an incomplete report submitted by the covered entity was in fact a covered cyber incident or reportable ransom payment. Finally, CISA believes this interpretation also is supported by the fact that CIR CIA authorizes CISA to issue a subpoena to “obtain the information required to be reported pursuant to section 681b of this title.” 6 U.S.C. 681d(c)(1). As the enforcement process requires the issuance of an RFI prior to the issuance of a subpoena, it is only logical that CISA would be able to issue an RFI for information it has the authority to request through a subsequent enforcement mechanism. For the same reason, CISA interprets the language to allow for the issuance of an RFI when CISA believes an entity has failed to submit a Supplemental Report as required.

2. Form and Contents of the RFI

Proposed § 226.14(c)(2) contains CISA’s proposal regarding the content CISA will include in an RFI. While not required to do so by the statute, CISA believes that enumerating the minimum content that CISA must include in an

RFI will help ensure that a covered entity receives information explaining why the RFI is being issued and the necessary elements for the covered entity’s response to be adequate. CISA proposes that an RFI must include the covered entity’s contact information; a summary of the facts describing CISA’s reason to believe that the covered entity failed to report a covered event in compliance with the regulation; a description of other requested information to allow CISA to confirm whether a reportable event occurred; the form in which information must be provided; and the date the information is due. As set forth in proposed § 226.14(c)(2), CISA interprets “information” broadly, including, among other things, tangible items, electronically stored information, and verbal or written responses.

In certain cases, CISA may want to issue an RFI based on facts that are derived from nonpublic, confidential, or classified information, sources, or processes. CISA is proposing in § 226.14(c)(2)(ii) and (f) that, in such a case, CISA will not reveal the nonpublic, confidential, or classified information, sources, or processes, and may limit the summary of the facts to a statement that CISA is aware of facts indicating that the covered entity has failed to report a covered cyber incident or ransom payment as required.

3. RFI Response

Proposed § 226.14(c)(3) states that a covered entity must reply in the manner and format, and within the deadline, set forth in the RFI. If the covered entity’s response to the RFI is inadequate, the Director, or Director’s designee, may request additional information from the covered entity to determine whether a covered cyber incident or ransom payment occurred, or the Director may issue a subpoena to compel the provision of information. Examples of an inadequate response to an RFI include, but are not limited to, failing to respond to the RFI, providing a response with insufficient information for CISA to confirm that a covered cyber incident or ransom payment occurred, or a covered entity’s continued failure to comply with the mandatory covered cyber incident, ransom payment, and/or Supplemental Report reporting obligations set forth in § 226.3.

4. Treatment of Information Received

Under 6 U.S.C. 681d(b)(2), information provided to CISA in response to an RFI is to be treated as if it was submitted through the standard reporting procedures established for submission of a CIR CIA Report. As a

result, information submitted by a covered entity in response to an RFI receives the protections afforded by § 226.18 as well as the privacy and civil liberties procedures of § 226.19, to information submitted in a CIR CIA Report. This includes information provided to CISA in response to a request for additional information following a covered entity’s inadequate response to an RFI. CISA has included language in § 226.14(c)(4) of the proposed regulation confirming that the information protections that apply to information contained in CIR CIA Reports applies to information submitted in response to an RFI. As discussed below, however, these protections do not apply to information provided by the covered entity in response to a subpoena.

5. Unavailability of Appeal

CISA does not consider an RFI to constitute a final agency action. RFIs have no immediate regulatory implications for the entity, but rather are an interim step in CISA’s compliance communications with an entity and are not final agency action that has legal consequences for a party.³⁸⁴

In other words, the substance of any enforceable requirements triggering legal liability are not established by the RFI—any such requirements, if they are imposed, will not be established until CISA issues a subpoena for information. Consequently, the RFI is not final agency action. Pursuant to 5 U.S.C. 704, only final agency actions are subject to judicial review. Accordingly, as an RFI is not a final agency action, the issuance of an RFI cannot be appealed. CISA proposes including § 226.14(c)(5) to provide notice that the issuance of an RFI is not appealable.

iii. Subpoena

Pursuant to 6 U.S.C. 681d(c)(1), if the Director has not received an adequate response to an RFI within 72 hours of issuance of the RFI, the Director may issue to the covered entity a subpoena to compel disclosure of information deemed necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required within the applicable CIR CIA Report, as well as information necessary to assess potential impacts of the incident to

³⁸⁴ See *Bennett v. Spear*, 520 U.S. 154, 178 (1997) (agency action may not be interlocutory in nature, but must represent the “consummation of the agency’s decision making process” and be an action “by which rights or obligations have been determined or from which legal consequences will flow” (internal quotation marks omitted)).

national security, economic security, or public health and safety. CISA views the use of the word “may” in 6 U.S.C. 681d(c)(1) as providing the Director discretion in determining whether or not to issue a subpoena, and there could be times that the Director issues a second RFI if the covered entity’s reply was incomplete or unclear such that CISA cannot confirm whether or not a covered cyber incident or ransom payment has occurred. Proposed § 226.14(d)(1) codifies this in the regulation, articulating that the Director may issue a subpoena to compel disclosure of information from a covered entity if the entity fails to reply to an RFI or provides an inadequate response. CISA interprets “inadequate response” to mean the submission of a response to the RFI with omitted, incomplete, unclear, or otherwise insufficient answers to the Director’s, or Director’s designee’s, RFI. CISA also interprets “inadequate response” as including the covered entity’s continued failure to comply with the mandatory Covered Cyber Incident, Ransom Payment, and/or Supplemental Report reporting obligations set forth in 226.3.

1. Timing of Subpoena

Section 681d(c)(1) of title 6, United States Code, provides that the Director may issue a subpoena if a covered entity fails to respond to an RFI within 72 hours. CISA interprets this timeframe as the minimum period after which the Director may issue a subpoena. Thus, CISA is proposing to state in § 226.14(d)(2) that the Director may not issue a subpoena earlier than 72 hours after the date of service of an RFI. There is no deadline by which the Director must issue a subpoena; the Director may issue a subpoena any time after 72 hours from the date on which the Director issues an RFI.

2. Form and Contents of Subpoena

Proposed § 226.14(d)(3) contains CISA’s proposal regarding the content CISA will include in a subpoena. Similar to the form and content of an RFI, CISA believes that enumerating the minimum required content that must be included in a subpoena will help ensure that a covered entity receives information explaining why the subpoena is being issued and the requirements for an adequate response. CISA proposes a subpoena must include the name and address of the covered entity, an explanation of the basis for issuing the subpoena and a copy of the relevant RFI, a description of the information requested, the date by which the covered entity must reply, and the manner and form in which the

covered entity must provide the information to CISA. As in regard to the information that may be required in response to an RFI, CISA interprets “information” broadly here, including, among other things, tangible items, electronically stored information, and verbal or written responses.

In certain cases, CISA may want to issue a subpoena based on facts that are derived from nonpublic, confidential, or classified information, sources, or processes. CISA is proposing in § 226.14(d)(3)(ii) and (f) that, in such a case, CISA will not reveal the nonpublic, confidential, or classified information, sources, or processes, and may limit the summary of the facts to a statement that CISA is aware of facts indicating that the covered entity has failed to report a covered cyber incident, ransom payment, or substantial new or different information as required.

3. Reply to the Subpoena

Proposed § 226.14(d)(4) sets forth the subpoena response requirements for a covered entity. It states that the subpoenaed covered entity must respond by the deadline identified in the subpoena, and in the manner and format specified in the subpoena by the Director.

If the covered entity’s response to the subpoena is inadequate, the Director may request or subpoena additional information from the covered entity or request civil enforcement of the subpoena. Examples of inadequate response include, but are not limited to, a complete failure to respond, providing a response that does not allow CISA to determine whether a covered cyber incident or ransom payment occurred, providing a response that does not fully comply with the regulatory reporting requirements, or providing a response that is otherwise insufficient to assess the potential impacts to national security, economic security, or public health and safety. As further discussed below, information provided in response to a subpoena may be referred to the Attorney General for criminal prosecution or the head of a regulatory enforcement agency for enforcement if the Director believes that there is a basis for such action based on the information received.

CISA considers any responses to CISA’s subsequent engagement with a subpoenaed entity related to the covered cyber incident or ransom payment as subpoenaed information for the purpose of referral to the Attorney General or head of a regulatory agency and application of information protections. Thus, this information may be provided to the Attorney General or head of a

regulatory enforcement agency as discussed in § 226.14(d)(6)(ii) and is not entitled to the protections set forth in § 226.18. The Director will take into account the covered entity’s engagement and cooperation with CISA when determining whether to provide information to the Attorney General or head of a regulatory agency for criminal prosecution or regulatory enforcement, respectively, or to pursue civil enforcement.

4. Authentication Requirement for Electronic Subpoenas

Section 681d(c)(4)(A) of title 6, United States Code, states that any electronically issued subpoena must be authenticated with a cryptographic digital signature of an authorized representative of CISA, or other comparable technology, that allows CISA to demonstrate that CISA issued the subpoena and that the subpoena has not been altered or modified since its issuance. CISA will make available, for example on its website, information by which subpoena recipients can verify that the signature was provided by an authorized representative of CISA. A recipient of any electronically issued subpoena without the required authentication does not need to consider the subpoena to be valid. See 6 U.S.C. 681d(c)(4)(A). Proposed § 226.14(d)(5) reflects this requirement essentially verbatim. This authentication requirement applies solely to electronically issued subpoenas.

5. Treatment of Information Received in Response to a Subpoena

CIRCI provides a number of protections to information submitted to CISA voluntarily, as part of a compliant CIRCI Report, or in response to an RFI. These protections, all of which are mandated by CIRCI, are set forth in § 226.18 of the proposed regulation and described in Section IV.H.i in this document. CIRCI does not explicitly require similar protections be afforded to information provided in response to a subpoena issued under CIRCI. CISA is proposing to explicitly note in § 226.14(d)(6) of the regulation that these protections do not apply to information submitted in response to a subpoena. Similarly, CIRCI does not require that the privacy and civil liberties procedures apply to information provided in response to a subpoena issued under CIRCI, and thus CISA proposes to note explicitly in the regulatory text that these procedures do not apply to information submitted in response to a subpoena. The reason CISA is proposing that the CIRCI-

specific privacy and civil liberties procedures would not apply to responses to subpoenas is that such information is subject to different handling limitations and authorized uses than information received in a CIRCIA Report or in response to an RFI. Of note, subpoenaed information may be shared with certain law enforcement and regulatory officials. Although the CIRCIA-specific privacy and civil liberties procedures that CISA is proposing would not apply, CISA notes that any personal information contained in responses to subpoenas would still be handled in accordance with the Privacy Act of 1974³⁸⁵ and the E-Government Act of 2002.³⁸⁶

CISA is proposing this approach in the hopes that the unavailability of these protections for information submitted in response to a subpoena will serve as an incentive for covered entities to comply with the applicable regulation or an RFI, thus preventing the need for issuance of a subpoena. The RFI provides a window for covered entities that have failed to submit a CIRCIA Report, as required, to comply with their legal obligations. If the covered entity remedies their noncompliance at that time, the covered entity is entitled to protections under § 226.18 and procedures under § 226.19. If the entity remains noncompliant and CISA elects to issue a subpoena, any subsequent information provided by the covered entity in response to the subpoena will not benefit from those protections.

This section of the proposed regulation also includes language related to the Director's authority under 6 U.S.C. 681d(d)(1) to provide information submitted by a covered entity in response to a subpoena to the Attorney General or head of a Federal regulatory agency if the Director determines that the facts relating to the covered cyber incident or ransom payment may constitute grounds for criminal prosecution or regulatory enforcement action. As part of the decision-making process related to the exercise of this authority, the Director is allowed to consult with the Attorney General or the head of the appropriate Federal regulatory agency. See 6 U.S.C. 681d(d)(2). For reasons similar to those discussed in Section IV.G.ii.5 in this document above regarding the appealability of the issuance of an RFI, CISA proposes including in § 226.14(d)(6)(ii) a statement that any decision by the Director to execute this

authority is not a final agency action and cannot be appealed.

6. Withdrawal and Appeals of Subpoena Issuance

Section 226.14(d)(7)(i) provides that CISA, in its discretion, may withdraw a subpoena. If CISA withdraws a subpoena, CISA will serve the notice of withdrawal as set forth in § 226.14(e). Section 226.14(d)(7)(ii) addresses appeals of a subpoena issuance. CISA is proposing to allow covered entities to appeal the issuance of a subpoena within seven calendar days after the date of service by providing a written request to the Director to withdraw the subpoena. CISA is proposing requiring a Notice of Appeal to contain, at a minimum, the name of the covered entity appealing the subpoena issuance, the request that the Director withdraw the subpoena, the rationale for the request (*e.g.*, why the entity believes it is not a covered entity; why the entity believes that the incident is not a covered cyber incident), and any additional information the covered entity would like the Director to consider.

iv. Service of an RFI, Subpoena, or Notice of Withdrawal

Proposed § 226.14(e) sets forth the service process for an RFI, subpoena, or notice of withdrawal of a subpoena. CISA is proposing that these documents may be served on an officer, managing or general agent, or any other agent authorized by appointment or law to receive service or process, and that they may be served through a reasonable electronic or non-electronic means that demonstrates receipt, such as certified mail with return receipt, express commercial courier delivery, or electronic delivery. CISA further is proposing that the date of service of any RFI, subpoena, or notice of withdrawal of a subpoena shall be the date on which the document is mailed, electronically transmitted, or delivered in person, whichever is applicable. These proposed processes are consistent with standard processes used for service of legal documents.

v. Enforcement of Subpoenas

Pursuant to 6 U.S.C. 681d(c)(2)(A), if a covered entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce the subpoena. A civil action to enforce a subpoena under CIRCIA may be brought in any judicial district in which the covered entity against whom the action is brought resides, is found, or does

business. 6 U.S.C. 681d(c)(2)(B). A court may punish a failure to comply with a CIRCIA subpoena as contempt of court. 6 U.S.C. 681d(c)(2)(C). CISA has proposed language reflecting these statutory authorities in § 226.15 of the proposed regulation.

The Director's referral of a subpoena to the Attorney General is discretionary. As discussed above, prior to making such a referral, the Director must consider, among other things, the covered entity's prior engagement with CISA.

vi. Acquisition, Suspension, and Debarment Enforcement Procedures

Section 681b(c)(8)(B)(ii) of title 6, United States Code, requires CISA to include in the final rule procedures related to "other available enforcement mechanisms including acquisition, suspension and debarment procedures." CISA is proposing procedures to effectuate this clause in §§ 226.16 and 226.17 of the proposed regulation.

Proposed § 226.16 would require the Director to refer all circumstances concerning a covered entity's noncompliance that may warrant suspension and debarment action to the DHS Suspension and Debarment Official. Suspension and debarment are meant to help protect the Federal government from fraud, waste and abuse by supporting the Federal government's ability to avoid doing business with non-responsible contractors.³⁸⁷ By including this requirement in CIRCIA, Congress has provided CISA with an enforcement mechanism to both discourage and, when necessary, punish noncompliance by making it more difficult for entities who meet the standard for suspension and debarment to do business with the Federal government.

Proposed § 226.17 address the "acquisition" portion of 6 U.S.C. 681b(c)(8)(B)(ii), by authorizing the Director to provide information regarding a noncompliant entity who has a procurement contract with the Federal government to the contracting official responsible for oversight of the contract in question and to the Attorney General. Whether or not any action can or should be taken against the entity who is the subject of the referred information is up to the contracting official's Department or Agency or the Attorney General, not CISA.

³⁸⁷ See GSA, *Frequently Asked Questions: Suspension & Debarment*, <https://www.gsa.gov/policy-regulations/policy/acquisition-policy/office-of-acquisition-policy/gsa-acq-policy-integrity-workforce/suspension-debarment-and-agency-protests/frequently-asked-questions-suspension-debarment> (last visited Nov. 28, 2023).

³⁸⁵ See 5 U.S.C. 552a.

³⁸⁶ See 44 U.S.C. 3501 note, Public Law 107-347.

vii. Penalty for False Statements and Representations

Any person that knowingly and willfully makes a materially false or fraudulent statement or representation in connection with, or within, a CIRCIA Report, RFI Response, or reply to an administrative subpoena is subject to penalties under 18 U.S.C. 1001. CISA interprets materially false or fraudulent statements or representations relating to CIRCIA to potentially include, but not be limited to, knowingly and willfully doing any of the following: submitting a CIRCIA Report for an incident that did not occur, claiming to be a representative of a covered entity whom you do not in fact represent, certifying you are a third party authorized to submit on behalf of a covered entity when you do not have authorization, and including false information within a CIRCIA Report, RFI Response, or response to an administrative subpoena. CISA would not consider scenarios where a covered entity reports information that it reasonably believes to be true at the time of submission, but later learns through investigation that it was not correct and submits a Supplemental Report reflecting this new information, to constitute a false statement or representation. Penalties for making false statements and representations under 18 U.S.C. 1001 include a fine or imprisonment for not more than five years. The maximum penalty for making false statements and penalties increases to eight years imprisonment if the false statement is related to international or domestic terrorism or certain sexual offenses. As part of implementing this proposed provision, CISA would refer potential violations of this proposed provision to DOJ, and DOJ would determine whether to prosecute violators of 18 U.S.C. 1001. Further, the inclusion of materially false or fraudulent statements or representations in submissions to CISA would not receive the protections and restrictions on use enumerated in § 226.18 because they would be inaccurate, incomplete, or invalid submissions that do not satisfy the regulatory reporting obligations and requirements proposed by this Part.

viii. Request for Comments on Proposed Enforcement

CISA seeks comments on its proposed approach to enforcement and noncompliance, including the following:

62. The proposed approach for RFIs, to include the delegation of authority to issue an RFI; the circumstances in which an RFI should be issued; the form

and content of an RFI; the manner, form, and timeline for responding to an RFI; the treatment of information received in response to an RFI; and the lack of availability of an appeal for an RFI;

63. The proposed approach for subpoenas, to include the circumstances in which a subpoena should be issued; the timing of issuance of a subpoena; the form and content of a subpoena; the manner, form, and timeline for responding to a subpoena; the treatment of information received in response to a subpoena; and the withdrawal and appeal of a subpoena;

64. The proposed service process for an RFI, Subpoena, or Notice of Withdrawal;

65. The proposed process for enforcement of subpoenas, to include the referral of the matter to the Attorney General to bring a civil action; and

66. The proposed acquisition, suspension, and debarment enforcement procedures.

H. Protections

i. Treatment of Information and Restrictions on Use

1. Overview

CIRCIA applies a variety of information protections and restrictions on the use of CIRCIA Reports, as well as information submitted in response to an RFI. See 6 U.S.C. 681d(b)(2), 681e(b), 681e(a)(1) and (5). CIRCIA also provides liability protection for any person or entity that submits a CIRCIA Report in compliance with the reporting requirements established in the CIRCIA regulation or in a response to an RFI, as described in greater detail below. See 6 U.S.C. 681e(c). To ensure that the full suite of information protections and restrictions on use of CIRCIA Reports authorized by CIRCIA applies consistently to CIRCIA Reports or information in CIRCIA reports (as applicable), as well as responses to RFIs, CISA proposes to include them in § 226.18 of the proposed rule. However, as discussed in the section on Treatment of Information Received in Response to a Subpoena (Section IV.G.iii.5 in this document), CIRCIA does not require similar protections to be afforded to information provided in response to a subpoena issued under CIRCIA. Therefore, CISA proposes to specifically exclude all information and reports submitted in response to a subpoena from receiving any of the protections provided under § 226.18 of the proposed rule.

Consistent with 6 U.S.C. 681e, § 226.18 generally includes protections governing how CIRCIA Reports or the information submitted therein and

responses to RFIs must be treated within the U.S. Government and restricts how CIRCIA Reports or the information submitted therein and responses to RFIs may be used. The proposed rule separates these protections into two broad categories with the specific protections afforded to (1) CIRCIA Reports or information submitted in CIRCIA Reports and responses to RFIs and (2) reporting entities and persons detailed under each. Specifically, CISA proposes under the first category, Treatment of Information, the following protections which are consistent with 6 U.S.C. 681e: (a) Designation as Commercial, Financial, and Proprietary Information, (b) Exemption from Disclosure under FOIA, (c) No Waiver of Privilege or Protection Provided by Law, and (d) an Ex Parte Communications Waiver. Under Restrictions on Use, CISA proposes the following restrictions consistent with 6 U.S.C. 681e: (a) Prohibition on Use in Regulatory Actions, (b) Liability Protection and Evidentiary and Discovery Bar for CIRCIA Reports, and (c) Authorized Uses. CISA's understanding and interpretation of each of these protections and restrictions is provided in more detail below. Consistent with 6 U.S.C. 681e, § 226.18(a) notes that each provision of § 226.18 applies to CIRCIA Reports or the information in CIRCIA Reports, as stated in the respective subsection.

2. Treatment of Information

a. Designation as Commercial, Financial, and Proprietary Information

Consistent with 6 U.S.C. 681e(b)(1), § 226.18(b)(1) provides that a covered entity may designate a CIRCIA Report, a response to an RFI, or any portion thereof, as commercial, financial, and proprietary information by clearly designating the report or a portion thereof as such with appropriate markings at the time of submission. CISA intends to enable covered entities or third parties to easily perform this designation when submitting a CIRCIA Report by including in the web-based form for all CIRCIA Reports a mechanism such as a check box through which such a designation can be made. Upon a covered entity or third-party submitter making the designation, CISA will treat the CIRCIA Report, or the designated portions thereof, as commercial, financial, and proprietary information belonging to the covered entity.

b. Exemption From Disclosure Under FOIA

Consistent with 6 U.S.C. 681e(b)(2), § 226.18(b)(2) provides that CIRCIA Reports and responses to RFIs submitted in compliance with the CIRCIA regulation are exempt from disclosure under section 552(b)(3) of the FOIA and any State, Local, or Tribal government freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records. CISA proposes that, in the event CISA receives a FOIA request for which a CIRCIA Report or response to RFI would be responsive, CISA would assert that this exemption from disclosure under FOIA applies to such CIRCIA Report or response to RFI if submitted by a covered entity or third-party submitter in conformance with the manner, form, and content requirements described in §§ 226.6 through 226.11. CISA does not see any compelling policy reason or legal rationale to interpret this CIRCIA statutory exemption from disclosure under the FOIA any differently than as the plain language states and interprets the CIRCIA FOIA exemption to protect against disclosure of CIRCIA Reports and responses to RFIs. Further, if CISA receives a FOIA request for a CIRCIA Report, response to RFI, or information contained therein, CISA will apply any other applicable exemptions, consistent with DHS FOIA regulations.

c. No Waiver of Privilege

Consistent with 6 U.S.C. 681e(b)(3), § 226.18(b)(3) provides that a covered entity does not waive any applicable privilege or protection provided by law, including trade secret protection, as a consequence of submitting a CIRCIA Report or response to an RFI in conformance with the CIRCIA regulations. Accordingly, to the extent that any claim of a waiver is based on disclosure of the information to the Federal government, CISA proposes to interpret the CIRCIA provisions to cover all circumstances where state or Federal privileges and protections may attach, including privileges or protections such as the attorney-client and work-product privileges, as well as others recognized under common law.

d. Ex Parte Communications Waiver

Consistent with 6 U.S.C. 681e(b)(4), § 226.18(b)(4) provides that CIRCIA Reports and responses to RFIs submitted in conformance with the CIRCIA regulation are not subject to the rules or procedures of any Federal agency or department or any judicial doctrine

regarding ex parte communications with a decision-making official, including any concerns about ex parte communications related to rulemaking or other processes under the Administrative Procedure Act, 5 U.S.C. 553 *et seq.* Consistent with this understanding, CISA proposes that the ex parte communications waiver offered by CIRCIA also extends to the procedures of any Federal agency or department regarding ex parte communications as CISA notes that not all Federal departments and agencies have rules that govern this issue.

3. Restrictions on Use

a. Prohibition on Use in Regulatory Actions

Consistent with 6 U.S.C. 681e(a)(5), proposed § 226.18(c)(1) provides that Federal and SLTT governments are prohibited from using information obtained solely through a CIRCIA Report submitted pursuant to the CIRCIA regulation or in a response to an RFI to regulate, including through an enforcement proceeding, the activities of a covered entity or any entity that made a ransom payment on behalf of a covered entity.³⁸⁸ CISA also proposes two exceptions to this prohibition that track 6 U.S.C. 681(a)(5)(A) and 681(a)(5)(B), respectively. First, CISA is proposing that information in CIRCIA Reports and responses to RFIs may be used to regulate if a Federal or SLTT Government entity expressly allows the covered entity to meet any separate regulatory reporting requirement that Federal or SLTT Government entity has in place through submission of CIRCIA Reports to CISA. Second, CISA is proposing that CIRCIA Reports and responses to RFIs may be used consistent with Federal or State authority specifically relating to the prevention and mitigation of cybersecurity threats to information systems to inform the development or implementation of regulation relating to such systems.

CISA views the first exception described above as applying to situations where a Federal or SLTT Government entity has independent regulatory authority to mandate reporting of covered cyber incidents or

³⁸⁸ CISA notes that cyber incident reporting that another agency separately obtains pursuant to reporting requirements issued under its own authorities, even if subsequently shared with CISA under an approved information sharing agreement (such as a CIRCIA Agreement), is not a "CIRCIA Report" as proposed to be defined in § 226.1. Therefore, such information is not obtained "solely" through a CIRCIA Report (even if separately obtained through a CIRCIA Report), and therefore is not subject to this bar.

ransom payments but has elected to streamline its own independent regulatory reporting requirements by allowing covered entities to submit such reports to CISA to satisfy both regulatory reporting requirements. Both currently and prior to the passage of CIRCIA, a small number of Federal regulators either direct or permit regulated entities to meet the respective regulator's cyber incident reporting requirements via reporting to CISA. For example, entities subject to TSA's cyber incident reporting requirements must report cybersecurity incidents to CISA via the internet reporting form or by telephone, and certain entities within the BES are required to provide cyber incident reports to both CISA and the Electricity ISAC. Pursuant to this exception, reports such as these, which are submitted to CISA by a covered entity in part to satisfy another independent regulatory reporting requirement, are permitted to be used by Federal and SLTT regulators for regulatory purposes, notwithstanding the otherwise generally applicable bar on regulatory use in § 226.18(c).

CISA notes that the second exception to the general prohibition on regulatory use of CIRCIA Reports and responses to RFIs is that they can provide Federal and SLTT government regulators with information to better understand the cyber threat landscape and the threats and trends that may be impacting the particular community that they are responsible for regulating.

b. Liability Protection

Consistent with 6 U.S.C. 681e(c)(1), proposed § 226.18(c)(2)(i) provides that no cause of action shall lie or be maintained in any court by any person for the submission of a CIRCIA Report submitted in conformance with the requirements of the CIRCIA regulation or response to an RFI and must be promptly dismissed by the court. Section 226.18(c)(2)(i) also clarifies the extent of this liability protection, which only applies to or affects civil litigation that is solely based on the submission of a CIRCIA Report or response to an RFI. This liability protection does not serve to shield covered entities from liability for the underlying covered cyber incident, ransomware attack, or ransom payment, should there be a separate basis for liability (*e.g.*, a violation of state consumer protection laws that was exploited by the cyber incident). Nor does the provision shield covered entities from liability for associated criminal acts. Additionally, § 226.18(c)(2)(iii) creates an exception that is consistent with 6 U.S.C. 681e(c)(3), which exempts actions taken

by the Federal government to enforce CIRCIA's reporting requirements as described in the enforcement Section IV.G in this document. Therefore, civil actions brought by the Federal government to enforce a subpoena are exempt from liability protection afforded under CIRCIA and may proceed in court.

Finally, § 226.18(c)(2)(ii) creates an evidentiary and discovery bar that prohibits CIRCIA Reports, responses to RFIs, and any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting CIRCIA Reports or responses to RFIs from being received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof. Consistent with 6 U.S.C. 681e(c)(3), § 226.18(c)(2)(ii) clarifies that the evidentiary and discovery bar created by CIRCIA does not create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting a CIRCIA Report or response to an RFI.

While the scope of the liability protection offered by CIRCIA is limited to litigation solely based on the submission of a CIRCIA Report, the submitted CIRCIA Report or response to an RFI itself is subject to a broad evidentiary and discovery bar. The scope of settings and venues for which this bar applies is broad—evidence, discovery, or other uses in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or any political subdivision. However, CISA notes that the scope of materials subject to this bar is narrow. Legislative history also makes clear that the intent was for this evidentiary and discovery bar to be limited to CIRCIA Reports, responses to RFIs, and the underlying materials created solely for the purpose of preparing, drafting, or submitting a CIRCIA Report or response to an RFI, but does not apply to the underlying information contained in the report or response. Based on this understanding of legislative intent and a plain reading of CIRCIA, CISA understands this to mean that while a CIRCIA Report or response to an RFI could not, for example, be attached to a warrant application, the underlying information contained in the CIRCIA Report or response to an RFI could be used to support the warrant application.

Further, CISA cannot provide a CIRCIA Report or response to an RFI in response to a third-party discovery request. Similarly, the protection for other records is limited only to those created solely to facilitate preparing, drafting, or submitting a report; this would include, for example, a draft submission, or an email seeking to verify information for the express purpose of populating a CIRCIA Report or response to an RFI. However, a forensic incident report that was developed for the purpose of investigating the underlying incident, which happened to have been used in populating a CIRCIA Report or response to an RFI, would not be “created for the sole purpose of preparing, drafting, or submitting” a CIRCIA Report or response to an RFI. Therefore, CISA's view is that this bar would not create a defense to discovery for a record, such as the forensic record example above, that was not created for the sole purpose of preparing, drafting, or submitting a CIRCIA Report or response to an RFI.

c. Limitations on Authorized Uses

Consistent with 6 U.S.C. 681e(a)(1), CISA proposes including a section in the regulations identifying the statutory limitations on the uses of information provided to CISA in a CIRCIA Report or response to an RFI. Specifically, proposed § 226.18(c)(3) generally states that information provided to CISA in a CIRCIA Report or response to an RFI may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal government solely for the delineated purposes. These purposes are generally consistent with the authorized use limitations for cyber threat indicators and defensive measures shared with the Federal government under the Cybersecurity Act of 2015 (6 U.S.C. 1501–1533), with the additional authorized purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of events required to be reported in accordance with § 226.3.³⁸⁹ This additional authorized purpose would allow, for example, information provided to CISA in a CIRCIA Report or response to an RFI to be used by Federal law enforcement agencies to investigate, identify, capture, and prosecute perpetrators of cybercrime. In light of the often

³⁸⁹ This includes, for example, the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, serious bodily harm, or serious economic harm, which CISA interprets to include a terrorist act or use of a weapon of mass destruction.

interconnected nature of cyber incidents and cyber campaigns, and the resulting holistic response actions that the Federal government may take to respond to such cyber incidents and campaigns, CISA views the proposed term “events” in proposed § 226.18(c)(3)(v)(A) to broadly to include events such as campaigns, individual cyber incidents, or otherwise related cyber incidents. CISA therefore interprets the statutory provision as authorizing the Federal government to use all of the information about cyber incidents provided to CISA in accordance with proposed § 226.3 or voluntarily for this additional authorized purpose. While not separately defined in the regulation, CISA understands “cybersecurity purpose” and “security vulnerability” to have the meaning given those terms in the Homeland Security Act of 2002, as amended, specifically at 6 U.S.C. 650.³⁹⁰

ii. Protection of Privacy and Civil Liberties

CIRCIA requires that the rule include procedures for protecting privacy and civil liberties consistent with processes adopted pursuant to 6 U.S.C. 1504(b) and for anonymizing and safeguarding, or no longer retaining information received through CIRCIA Reports that is known to be personal information that is not directly related to a cybersecurity threat. See 6 U.S.C. 681b(c)(8)(D). CISA is proposing to include these procedures in § 226.19, and they would apply to personal information in CIRCIA Reports, as well as in information submitted in response to an RFI. CISA is proposing to place privacy controls and safeguards at the point of receipt of a CIRCIA Report as well as for the retention, use, and dissemination of a CIRCIA Report. CISA proposes that the procedures proposed in this section will not apply, however, to information and reports submitted in response to a subpoena. Although the CIRCIA-specific privacy and civil liberties procedures that CISA is proposing would not apply to subpoenaed information, CISA notes that information contained in responses

³⁹⁰ 6 U.S.C. 650(6) defines “cybersecurity purpose” as “the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.” 6 U.S.C. 650(25) defines “security vulnerability” as “any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.” In turn, 6 U.S.C. 650(24) defines “security control” as “the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.”

to subpoenas would still be handled in accordance with the Privacy Act of 1974³⁹¹ and the E-Government Act of 2002.³⁹²

1. Instructions for Personal Information

CISA is proposing steps to minimize the collection of unnecessary personal information in CIRCIA Reports and in responses to RFIs. First, CISA is proposing that covered entities should only include personal information that is requested in the reporting form or in the RFI and should exclude any unnecessary personal information. CISA would include on the CIRCIA Incident Reporting Form instructions and guidance on when personal information should and should not be included in a CIRCIA Report. While some personal information, such as the contact information for the covered entity and information about the identity of the actor perpetrating the incident (if known), will be required for the CIRCIA Incident Reporting Form, CISA will endeavor to provide clear guidance to help covered entities avoid submitting extraneous personal information. For example, while the CIRCIA Report would require categories of information that were believed to have been accessed or acquired by an unauthorized person, CISA would provide guidance that CIRCIA Reports should not include any specific personal information that was accessed. Thus, while a covered entity might indicate whether, for example, medical or driver's license information was accessed in the incident, the covered entity should not provide the medical information itself nor a list of the compromised driver's license numbers or images.

CISA would also include privacy-preserving measures in the CIRCIA Incident Reporting Form tool itself to help prevent covered entities from including unnecessary personal information. Such measures could include limiting the number of fields requiring open-ended responses, as well as mechanisms to scan for indicators that unnecessary personal information might be included (*e.g.*, information in standard social security number format) and prompts for the covered entity to verify whether the information is necessary to submit before proceeding with the report submission.

CISA considered, but is not proposing, prohibiting submission of unnecessary personal information in CIRCIA Reports. The Cybersecurity Act of 2015 includes a provision that

requires non-Federal entities to review cyber threat indicators before submission to CISA to assess whether those indicators contain any information not directly related to a cybersecurity threat that the entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information. See 6 U.S.C. 1502(b). Although a requirement to remove irrelevant personal information would likely reduce the amount of personal information collected through CIRCIA Reports, CISA is not proposing this option due to the increased burden such a requirement would likely place on compliance with CIRCIA reporting requirements. Because such a prohibition would likely have required that CISA reject reports that include such information or otherwise determine that the report was not correctly submitted, such a prohibition would place a greater burden on covered entities to comply with CIRCIA reporting requirements and would likely make meeting the required report submission timelines more difficult. CISA welcomes comment on these and any other steps that could reduce the collection of unnecessary personal information.

2. Assessment of Personal Information

CISA is proposing to review each CIRCIA Report to determine if the report contains personal information other than the personal information specifically requested. Because some fields in the CIRCIA Incident Reporting Form specifically ask for personal information, such as covered entity contact information and certain information about the threat actor (if known), CISA would assume that those fields in a submitted CIRCIA Report contain personal information, and would not necessarily review those fields, though CISA may do so to determine if extraneous personal information might have been included. CISA would then assess the personal information to determine if it is directly related to a cybersecurity threat, as that term is proposed to be defined in proposed § 226.1. personal information that is necessary to detect, prevent, or mitigate a cybersecurity threat would be considered directly related to a cybersecurity threat. Examples of personal information directly related to a cybersecurity threat would include malicious IP addresses, spoofed email addresses, domains that contain names from which malicious emails were sent, compromised usernames, and spoofed identities in malicious emails. Examples

of personal information that would typically not be directly related to a cybersecurity threat would include contact information of the victim or entity reporting on behalf of the victim, and the name of a recipient of a malicious email.

CISA would automate its reviews for personal information to be automated to the extent practicable taking into consideration costs, technical complexities, and any other challenges associated with automation, and to use human review when necessary. Privacy controls and safeguards include the internal administrative, technical, and physical safeguards that CISA employs to ensure compliance with privacy requirements and manage privacy risks. Examples of the controls CISA would employ include ensuring only those who have a need to know can access, retain, or disseminate covered reports; ensuring those with a need to know are trained on proper handling procedures; and that activities using CIRCIA Reports are solely used for purposes in which the CIRCIA Report was first collected.

When CISA determines that personal information submitted in a CIRCIA Report is not directly related to a cybersecurity threat, CISA proposes to delete the information, unless it is necessary contact information. For personal information necessary for contacting the covered entity or the report submitter, CISA proposes to safeguard and anonymize the information prior to sharing the report outside of the Federal government, unless CISA receives the consent of the individual to share their personal information and the personal information can be shared without revealing the identity of the covered entity. CISA proposes to retain personal information that is directly related to a cybersecurity threat and may share such personal information consistent with the provisions of section 226.18 and the privacy and civil liberties guidance, which is described below.

Consistent with the approach to privacy and civil liberties protections in 6 U.S.C. 1504(b), CISA is proposing to develop and publish privacy and civil liberties guidance that would apply to CISA's retention, use, and dissemination of personal information contained in a CIRCIA Report, and which would also provide guidance to other Federal departments and agencies with which CISA shares CIRCIA Reports. The guidance is not intended to place any requirements on regulated entities. CISA would draft the guidance to be consistent with the need to protect personal information from unauthorized use or disclosure and mitigate

³⁹¹ See 5 U.S.C. 552a.

³⁹² See 44 U.S.C. 3501 note, Public Law 107-347.

cybersecurity threats; thus, in the guidance, CISA would endeavor to balance the privacy and civil liberties concerns relating to the handling of personal information with the need, where applicable, for personal information to address cybersecurity threats.

In the guidance, CISA would describe how CISA would review reports to identify personal information and to determine whether the information is or is not related to a cybersecurity threat. CISA would also plan to describe in the guidance the use of technical capabilities to remove or anonymize personal information not directly related to a cybersecurity threat. CISA would also describe a process for the timely destruction of personal information that is not directly related to a cybersecurity threat and that is not contact information needed to contact the submitter or covered entity.

CISA would make the guidance publicly available, likely by publishing the guidance on its website at the same time as the publication of the final rule for this rulemaking. CISA proposes to review the effectiveness of the guidance one year after publication to ensure it is appropriate to the needs for retention, use, and dissemination of personal information for mitigation and protection against cybersecurity threats and appropriately protect privacy and civil liberties of individuals. CISA proposes to conduct periodic subsequent reviews after the initial review. The CISA Chief Privacy Officer will also conduct an initial review of CISA's compliance with the guidance after one year and subsequent periodic reviews not less than every three (3) years. Where reviews result in a change needed to the guidance, CISA would publish updated guidance on its website.

CISA has included draft guidance in the docket for this proposed rule and is accepting public comment on any aspect of the draft guidance.

iii. Digital Security

CISA recognizes that reports submitted under CIRCIA and responses to RFIs often will include sensitive security, business, or other confidential information. In addition to the legal protections described above that exist in part to ensure that sensitive information submitted in CIRCIA Reports and responses to RFIs is only shared with appropriate individuals or entities, CISA is committed to maintaining physical and cybersecurity measures in place to prevent illicit unauthorized access to the information CISA receives in CIRCIA Reports and responses to

RFIs. At a minimum, and consistent with 6 U.S.C. 681e(a)(4), CISA will ensure that CIRCIA Reports, responses to RFIs, and any information contained therein are collected, stored, and protected in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

iv. Request for Comments on Proposed Protections

CISA seeks comments on its proposed approach to the treatment of information, restrictions of use, and applicable protections, including the following:

67. The proposed approach to designating CIRCIA Reports, responses to RFIs, or the information contained therein as commercial, financial, and proprietary information;

68. The proposed application of the exemption from disclosure under FOIA and similar freedom of information laws;

69. The proposed implementation of the statement that submission of a CIRCIA Report or response to RFI does not waive any applicable privilege or protection;

70. The proposal that CIRCIA Reports and responses to RFIs are not subject to the rules governing ex parte communications;

71. The proposed restrictions on the use of information obtained solely through CIRCIA Reports or response to RFIs in regulatory actions or as independent causes of liability;

72. The proposed restrictions on the receipt of CIRCIA Reports or responses to RFIs in evidence, their discoverability, or their other use in any trial, hearing, or similar proceeding; and

73. The proposed privacy and civil liberties protections, to include the steps proposed by CISA to minimize the collection of unnecessary personal information in CIRCIA Reports, the assessment of personal information contained therein, and the draft guidance CISA is proposing to create.

I. Severability

To the extent that any portion of this proposed rule becomes final and is declared unenforceable by a court, CISA has structured the proposed rule so that all remaining provisions are severable from each other to the extent practicable and remain in effect unless they are dependent on the vacated or enjoined provision. Thus, even if a court decision invalidating or vacating a portion of the CIRCIA final rule results in a partial amendment to the regulation or a

reversion to the statutory language itself, CISA intends that the rest of the rule continue to operate.

V. Statutory and Regulatory Analyses

A. Regulatory Planning and Review

Executive Orders 12866, Regulatory Planning and Review,³⁹³ as amended by Executive Order 14094, Modernizing Regulatory Review,³⁹⁴ and 13563, Improving Regulation and Regulatory Review,³⁹⁵ direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, reducing costs, harmonizing rules, and promoting flexibility.

The Office of Management and Budget (OMB) has designated this rule a "significant regulatory action" as defined under section 3(f)(1) of E.O. 12866, as amended by Executive Order 14094, because its annual effects on the economy would exceed \$200 million in at least one year of the analysis. Accordingly, OMB has reviewed this proposed rule.

CISA has prepared a Preliminary Regulatory Impact Analysis (RIA) which can be found in the docket for this proposed rule. CISA welcomes comment on the Preliminary RIA, and includes a summary of findings below.

Through this NPRM, CISA proposes the following reporting requirements, collectively known as CIRCIA Reports:

- A covered entity that experiences a covered cyber incident must report that incident to CISA no later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.
- A covered entity that makes a ransom payment, or has another entity make a ransom payment on its behalf, as the result of a ransomware attack against the covered entity must report that payment to CISA no later than 24 hours after the ransom payment has been disbursed.
- A covered entity that experiences a covered cyber incident and makes a

³⁹³ See E.O. 12866, *Regulatory Planning and Review*, 58 FR 190 (Oct. 4, 1993), available at http://www.reginfo.gov/public/jsp/Utilities/EO_12866.pdf.

³⁹⁴ See E.O. 14094, *Modernizing Regulatory Review*, 88 FR 21879 (Apr. 11, 2023), available at <https://www.govinfo.gov/content/pkg/FR-2023-04-11/pdf/2023-07760.pdf>.

³⁹⁵ See E.O. 13563, *Improving Regulation and Regulatory Review* (Jan. 18, 2011), available at http://www.reginfo.gov/public/jsp/Utilities/EO_13563.pdf.

ransom payment, or has another entity make a ransom payment on its behalf, that is related to the covered cyber incident may report both events to CISA in a joint report no later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

- A covered entity must promptly submit a Supplemental Report about a previously reported covered cyber incident if substantial new or different information becomes available.
- A covered entity must submit a Supplemental Report if the covered entity makes a ransom payment, or has another entity make a ransom payment on its behalf, that relates to a covered cyber incident that was previously reported. The covered entity must submit the Supplemental Report to

CISA no later than 24 hours after the ransom payment has been disbursed.

In addition to reporting, CISA proposes data and records preservation requirements, which would require that certain data and records related to reported covered cyber incidents and ransom payments be maintained beginning on the date upon which the covered entity establishes reasonable belief that a covered cyber incident occurred or the date upon which a ransom payment was disbursed and until two years following the last report submitted to CISA. This data and records preservation is essential to enabling investigation of cyber incidents.

CISA estimates that the total affected population of this proposed rule would be 351,383 covered entities based on the

above criteria. However, due to overlap across the sector criteria as well as overlap between the entities covered under both the sector-based criteria and the size-based criterion (*i.e.*, all large entities that are also captured under the sector-based criteria), CISA believes that this affected population represents an overestimate of the number of covered entities. As such, CISA assumes that there would be a 10% overlap, which has been removed from the total number of the affected population. Table 1 below presents the total affected population by covered entity³⁹⁶ criteria and the 10% reduction for the affected population.³⁹⁷ For the rest of this analysis, CISA based its estimates on 316,244 covered entities, accounting for the 10% overlap.

TABLE 1—AFFECTED POPULATION, BY CRITERIA

Criteria	Affected population	
	Total	Excluding the 10% overlap
Non-Small Entities	35,152	31,637
Sector-Based Criteria		
Owns or Operates a Covered Chemical Facility	3,249	2,924
Provides Wire or Radio Communications Service	71,250	64,125
Owns or Operates Critical Manufacturing Sector Infrastructure	42,728	38,455
Provides Operationally Critical Support to the DoD or Processes, Stores, or Transmits Covered Defense Information	80,000	72,000
Performs an Emergency Service or Function	9,257	8,331
Bulk Electric and Distribution System Entities	4,214	3,793
Owns or Operates Financial Services Sector Infrastructure	42,965	38,669
Qualifies as an SLTT Government Entity	3,231	2,908
Qualifies as an Education Facility	13,421	12,079
Involved with Information and Communications Technology to Support Election Processes	106	95
Provides Essential Public Health-Related Services	14,418	12,976
IT Entities	6,708	6,037
Owns or Operates a Commercial Nuclear Power Reactor or Fuel Cycle Facility	107	95
Transportation System Entities	5,752	5,177
Subject to Regulation Under the Maritime Transportation Security Act	4,530	4,077
Owns or Operates a Qualifying Community Water System or Publicly Owned Treatment Works	14,295	12,866
Total ³⁹⁸	351,383	316,244

The Preliminary RIA estimates the costs of complying with the proposed requirements for an affected population of 316,244 covered entities over the period of analysis.³⁹⁹ The main industry cost drivers of this proposed rule are the costs associated with becoming familiar with the rule, data and records

preservation, and reporting requirements. Other costs include those associated with help desk calls and enforcement actions. Although this analysis uses a base year of 2024, CISA estimates industry costs beginning in 2025 upon the expected publication of the Final Rule. The combined cost of the

NPRM is based on an 11-year period of analysis, as CISA estimates government costs starting in 2023 to account for costs incurred before the expected publication of the final rule, which is covered under the pre-regulatory

³⁹⁶ This table identifies the covered entities that would be required to comply with the rule. In addition to these entities, CISA estimates that an additional approximately 13 million entities would not actually be covered entities but would still incur some burden to determine they are not covered entities. This is detailed in Section 2 of the Preliminary RIA.

³⁹⁷ CISA does not expect there to be a 10% overlap uniformly across all sectors, but the overlap is applied uniformly for presentational purposes.

Since the costs do not differ across criteria or covered entities, there is no difference in applying the overlap to each sector as opposed to applying it to the total number of affected covered entities.

³⁹⁸ As discussed in Section 2.3 of the Preliminary RIA, CISA anticipates the total number of covered entities is an overestimate as some of the not-small entities would also be captured by the sector-based criteria. In addition, CISA anticipates there to be overlap across the sector-based criteria. For example, the 80,000 DoD contractors likely include

entities also captured under the critical manufacturing, transportation, and IT sectors. Other examples include likely overlap between the communications service providers and IT entities, and between CFATS and Maritime Transportation Security Act populations.

³⁹⁹ For the purposes of this analysis, CISA presents a static affected population over the period of analysis.

baseline costs, as discussed in the preliminary RIA.

Under this proposed rule, familiarization costs include the time spent by an entity in a critical infrastructure sector to review the rule and/or other materials to help the entity determine if it is a covered entity subject to the rule, as well as time spent by a covered entity reading the rule to understand the requirements imposed by the rule. Familiarization costs also include an annual burden for covered entities to review any necessary CIRCIA documents to ensure proper compliance. For the reporting requirements, covered entities would have to submit a CIRCIA Report if they experience a covered cyber incident or make a ransom payment as the result of a ransomware attack. The costs associated with these reporting requirements are the opportunity cost of time spent completing the forms, including preparation time to gather the necessary information to complete the forms. Data and records preservation costs include the time burden for data and information to be collected and placed into appropriate storage, either physical or digital, and storage costs the entity incurs that they would not have incurred but for the proposed CIRCIA data and records preservation requirements.

i. Number of Reports

CISA expects the Final Rule to publish in late 2025. In order to comply with Administrative Procedure Act and Congressional Review Act requirements, CISA would be required to delay the effective date of the rule for a total of 60 days, which would likely push the effective date to 2026. Due to this required delay and uncertainty surrounding the publication date, covered entities will likely not begin submitting CIRCIA reports until 2026. As such, reporting costs, and other associated costs, other than familiarization costs, will be estimated starting in 2026.⁴⁰⁰ Because there is a great deal of uncertainty regarding the number of CIRCIA Reports that would be required to be submitted upon implementation of this proposed rule, CISA presents a range for industry costs. As presented in the Preliminary RIA, CISA developed a sensitivity analysis for the range of expected number of CIRCIA Reports based on several sources, including current CISA

voluntary reporting through CISA's web-based Incident Reporting Form, reporting under DOD and DOE mandatory reporting programs, and cyber loss data from the Information Risk Insights Study (IRIS) 2022 by the Cyentia Institute,⁴⁰¹ which was sponsored by CISA. Using these sources to inform the percentage of covered entities expected to submit CIRCIA Covered Cyber Incident Reports, CISA applies percentages of 2%, 5%, and 10% to the total affected population to conduct our low, primary, and high estimates for the number of cyber incidents that would need to be reported. These percentages were determined using the reporting rates from CISA, DoD, DOE, and the Cyentia Institute ranges as reference points. As none of the reporting populations discussed above are fully representative of the CIRCIA population of covered entities, CISA developed reporting percentages that present a reasonable range of possible outcomes. This takes into account the low reporting estimate of 0.725% for DoD DFARS reporting as well as the higher reporting ranges presented by Cyentia. Recognizing that the majority of entities that are proposed to be subject to the CIRCIA reporting requirements are small businesses through the sector-based criteria,⁴⁰² CISA determined that it was appropriate to present reporting percentages in line with the lowest revenue categories presented by Cyentia and not the high end of their range.

The number of Ransom Payment Reports is based on data from Federal Bureau of Investigation (FBI) annual internet crime reports regarding the number of ransomware attacks for which complaints are received annually. In the 2021 and 2022 reports, the FBI reports the number of voluntary complaints that indicated organizations in one of the 16 critical infrastructure sectors had been victims of a ransomware attack. The internet Crime Complaint Center received 649 such complaints in 2021,⁴⁰³ and 870 in 2022.⁴⁰⁴

⁴⁰¹ Cyentia Institute, *Information Risk Insights Study 2022*, tbl. 3, Loss Summary, available at <https://www.cyentia.com/iris-2022/>.

⁴⁰² According to the SBA, over 99% of all businesses are small businesses (see Section 2.1 of the Preliminary RIA). Additionally, the size standard criteria for covered entities represent approximately 6% of the regulated population, further supporting the assumption that the vast majority of covered entities would be considered small businesses.

⁴⁰³ FBI, Internet Crime Complaint Center, *Internet Crime Report 2021*, available at https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

⁴⁰⁴ FBI, Internet Crime Complaint Center, *Internet Crime Report 2022*, available at https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

Based on this limited data, CISA forecast the number of ransomware attacks in critical infrastructure sectors by estimating the linear trend in the data based on available data from 2021 and 2022.⁴⁰⁵ This results in an estimated 1,312 ransomware attacks that would be reported in 2024, which is Year 1 for this analysis, and an estimated 1,754 ransomware attacks in 2026, which is likely the first year in which covered entities would begin incurring reporting costs. CISA recognizes that not all ransomware attacks will result in a ransom payment being made; however, given the lack of a consensus regarding what percentage of ransomware attacks do result in a ransom payment, CISA has elected to provide a very conservative estimate and assume that all ransomware attacks result in ransom payments.

CISA bases the estimated number of Ransom Payment Reports on these values on the FBI internet Crime Complaint Center data.⁴⁰⁶ For the purposes of this analysis, CISA anticipates receiving Ransom Payment Reports from 2026 to 2033, which would be a total of 20,220 Ransom Payment Reports. CISA also makes assumptions regarding the number of Joint Covered Cyber Incident and Ransom Payment Reports. For the purposes of this analysis, CISA assumes a low estimate of 1%, a primary estimate of 2%, and a high estimate of 3% of covered entities submitting a Ransom Payment Report would submit a Joint Covered Cyber Incident and Ransom Payment Report.⁴⁰⁷

In addition to the ranges presented for Covered Cyber Incident Reports, CISA also developed a range of estimates for Supplemental Reports. CISA assumes the number of Supplemental Reports would be based on a percentage of entities submitting Covered Cyber Incident Reports and Joint Covered Cyber Incident and Ransom Payment Reports. Due to the lack of available data on how many Supplemental

www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

⁴⁰⁵ CISA conducted the forecast using Microsoft Excel's TREND function, which forecasts a linear trend based on the available data.

⁴⁰⁶ As reporting to the FBI internet Crime Complaint Center is voluntary, this may be an underestimate to the extent that it does not capture any non-reported ransomware attacks in critical infrastructure sectors; however, it may be an overestimate to the extent that it is capturing ransomware attacks that did not result in ransom payments.

⁴⁰⁷ The percentage of ransomware attacks that would be part of or would themselves be a covered cyber incident are based on CISA subject matter expertise. CISA requests comment on the number of Joint covered cyber incident and Ransom Payment Reports that would be filed.

⁴⁰⁰ For this analysis, CISA uses 2024 as Year 1 to account for initial government costs to implement the CIRCIA regulatory program, making 2026 year 3 of the analysis. CISA also includes government costs from 2023 as part of the pre-regulatory baseline.

Reports would need to be filed, CISA assumes 25% of entities submitting Covered Cyber Incident Reports and Joint Covered Cyber Incident and Ransom Payment Reports for the low estimate, 50% for the primary estimate, and 75% for the high estimate.⁴⁰⁸ These percentages for Supplemental Reports are applied to the range of covered

entities submitting Covered Cyber Incident Reports. For example, for each estimate in the range of covered cyber incidents (2%, 5%, and 10%), CISA applies the range of percentages of Supplemental Reports. Table 2 presents the range of Supplemental Reports for the primary estimate for this analysis, which applies the 50% of Covered

Cyber Incident and Ransom Payment Reports resulting in a Supplemental Report across the range of estimates.⁴⁰⁹

In Table 2, CISA presents the estimated number of CIRCIA Reports, by report type for the primary estimate, which is 210,525.

TABLE 2—NUMBER OF CIRCIA REPORTS, PRIMARY ESTIMATE

Year	Covered cyber incident reports	Ransom payment reports	Joint covered cyber incident and ransom payment reports	Supplemental reports	Total
2024	0	0	0	0	0
2025	0	0	0	0	0
2026	15,812	1,754	35	7,906	25,507
2027	15,812	1,975	40	7,921	25,748
2028	15,812	2,196	44	7,924	25,976
2029	15,812	2,417	48	7,926	26,203
2030	15,812	2,638	53	7,928	26,431
2031	15,812	2,859	57	7,930	26,659
2032	15,812	3,080	62	7,932	26,886
2033	15,812	3,301	66	7,935	27,114
Total	126,498	20,220	404	63,403	210,525

In Table 3, CISA presents the estimated range for the number of CIRCIA Reports that would be

submitted over the period of analysis, with a low estimate of 83,760, a primary estimate of 210,525, and a high estimate

of 463,850 over the period of analysis.⁴¹⁰

TABLE 3—NUMBER OF CIRCIA REPORTS

Year	Low estimate	Primary estimate	High estimate
2024	0	0	0
2025	0	0	0
2026	9,681	25,507	57,149
2027	9,905	25,748	57,377
2028	10,129	25,976	57,639
2029	10,353	26,203	57,872
2030	10,577	26,431	58,104
2031	10,800	26,659	58,337
2032	11,024	26,886	58,570
2033	11,291	27,114	58,802
Total	83,760	210,525	463,850

Note: Totals may not sum due to rounding.

ii. Industry Cost

The main costs to industry associated with this proposed rule are those associated with covered entities and entities that fall within a critical infrastructure sector that are not covered entities (hereinafter, “non-covered entities”) becoming sufficiently familiar with the rule to determine whether they are covered, and if it is determined that they meet one or more of the criteria for a covered entity, becoming familiar with

how to comply with the requirements. The second largest cost associated with this rule would be data and records preservation costs, followed by the cost for covered entities to complete the forms for the CIRCIA Reports (including preparation time). Covered Entities would also potentially incur costs associated with help desk calls and enforcement actions. For this analysis, all cost estimates are based on 2022 dollars.

Familiarization costs are estimated based on the opportunity cost of reading some or all of the rule or related materials to determine whether or not an entity is a covered entity, and if so, how to comply with the proposed rule. CISA estimates that covered entities would begin to incur familiarization costs upon publication of the Final Rule, with familiarization costs divided equally across years 2 and 3 of the

⁴⁰⁸ CISA requests comments on the number of Supplemental Reports that would be filed.

⁴⁰⁹ Section 3.1 of the Preliminary RIA presents the number of Supplemental Reports in greater

detail, breaking down the ranges for the low, primary, and high estimates for the number of reports submitted.

⁴¹⁰ Due to the high degree of uncertainty, CISA requests comment on the number of reports submitted, as well as the ranges used in this sensitivity analysis.

period of analysis.⁴¹¹ The Preliminary RIA presents a primary estimate of \$33.58 for a non-covered entity to determine that they are not a covered entity, and a primary estimate of \$1,587.49 for a covered entity to

familiarize themselves with the proposed rule. This cost per entity is based on personnel in either the lawyer or general manager labor category (or some combination thereof) spending 0.275 hours per non-covered entity and

13 hours per covered entity to review the rule or related materials. This per entity cost and the total cost is presented in Table 4.

TABLE 4—FAMILIARIZATION COST BY ENTITY TYPE, PRIMARY ESTIMATE

	Non-covered entities	Covered entities
Hourly Time Burden	0.275	13
Weighted Average Cost per Entity	\$33.58	\$1,587.49
Number of Entities	12,864,239	316,244
Total Cost	\$432,000,574	\$502,034,650

Note: Totals may not sum due to rounding.

In addition to initial familiarization costs for the affected population to read the rulemaking documents, CISA estimates an annual familiarization cost for covered entities to review CIRCIA program information. CISA bases this cost on each covered entity having a staff member equivalent to a General

and Operations Manager spending 30 minutes (0.5 hours) reviewing the CIRCIA reporting forms, CIRCIA definitions, or any other information to ensure they are prepared to comply with the requirements if necessary. At an hourly compensation rate of \$102.42,

the per-entity cost is estimated to be \$51.21.⁴¹²

Combining the primary cost estimate for initial familiarization with the annual familiarization costs results in a total cost of \$1.1 billion over the period of analysis, as presented in Table 5.

TABLE 5—TOTAL FAMILIARIZATION COSTS
[\$ Millions, undiscounted]

Year	Initial familiarization		Annual familiarization	Total
	Non-covered entities	Covered entities		
2024	\$0	\$0	\$0	\$0
2025	251.0	216.0	0.0	467.0
2026	251.0	216.0	8.1	475.1
2027	0.0	0.0	16.2	16.2
2028	0.0	0.0	16.2	16.2
2029	0.0	0.0	16.2	16.2
2030	0.0	0.0	16.2	16.2
2031	0.0	0.0	16.2	16.2
2032	0.0	0.0	16.2	16.2
2033	0.0	0.0	16.2	16.2
Total	502.0	432.0	121.5	1,055.5

Note: Totals may not sum due to rounding.

The reporting cost is estimated based on the time spent completing the CIRCIA Reports. CISA estimates that both Covered Cyber Incident and Ransom Payment Reports would take three hours to complete, a Joint Covered Cyber Incident and Ransom Payment

Report would take 4.25 hours to complete, and a Supplemental Report would take 7.5 hours to complete. As described in the Preliminary RIA, CISA assumes a weighted average compensation rate of \$86.29 for the personnel responsible for completing

the report. Multiplying this compensation rate by the time burden and number of reports from the primary estimate results in an estimated cost of \$79.1 million for CIRCIA Reports, as presented in Table 6.

⁴¹¹ Some covered entities could begin reviewing and familiarizing themselves with the Final Rule upon publication in late 2025, before the effective date, which would likely not be until 2026 due to

required delays for major rules associated with the Administrative Procedure Act and Congressional Review Act. Other covered entities could wait until the effective date.

⁴¹² \$51.21 per entity = 0.5 hours × \$102.42 per hour. Information on the hourly compensation rates used is contained in Section 3.2 of the Preliminary RIA.

TABLE 6—COST OF CIRCIA REPORTING

Year	Covered cyber incident reports	Supplemental reports	Ransom payment reports	Incremental cost of joint covered cyber incident and ransom payment reports	Total
2024	\$0	\$0	\$0	\$0	\$0
2025	0	0	0	0	0
2026	4,093,099	5,116,373	454,035	3,784	9,667,290
2027	4,093,099	5,126,294	511,242	4,260	9,734,895
2028	4,093,099	5,127,724	568,449	4,737	9,794,009
2029	4,093,099	5,129,154	625,657	5,214	9,853,123
2030	4,093,099	5,130,584	682,864	5,691	9,912,237
2031	4,093,099	5,132,015	740,071	6,167	9,971,352
2032	4,093,099	5,133,445	797,279	6,644	10,030,466
2033	4,093,099	5,134,875	854,486	7,121	10,089,580
Total	32,744,788	41,030,464	5,234,082	43,617	79,052,951

CISA also estimates costs associated with Data and Records Preservation. CISA estimates that a covered entity would spend six hours per submission to collect, store, and maintain records in the first year of the preservation period.⁴¹³ The cost of this provision is based on an hourly compensation rate of \$35.19, which is the rate for Office and Administrative Support.⁴¹⁴ Based on six hours per year, at \$35.19 per hour, the annual labor cost of data and record preservation would be \$211.12.

CISA also estimates costs associated with acquiring additional storage to save

records related to CIRCIA Reports. According to CISA Cybersecurity Division, a cyber incident generates four terabytes of data, on average.⁴¹⁵ To estimate the cost of storage for this amount of data, CISA conducted market research to determine the cost of sufficient cloud storage to store and access the data. Based on this research, the price of cloud storage for four terabytes of data would have an annual cost ranging from under \$700 to almost \$1,300.⁴¹⁶ Based on this range, CISA assumes that all covered entities that submit a CIRCIA Report would spend

\$1,000 per year on cloud storage for two years.⁴¹⁷ Applying the \$1,000 cost for data and record preservation for the number of reports for two years results in a storage cost range of \$132.4 million to \$512.6 million, with a primary estimate of \$275.1 million over the period of analysis.

Combining the labor and storage costs results in a total data and record preservation cost range from \$147.4 million to \$570.4 million, with a primary estimate of \$306.1 million, as presented in Table 7.

TABLE 7—DATA AND RECORD PRESERVATION COSTS

Year	Low estimate	Primary estimate	High estimate
2024	\$0	\$0	\$0
2025	0	0	0
2026	9,805,715	21,317,218	40,488,895
2027	18,172,475	39,191,526	74,195,639
2028	18,666,018	39,689,956	74,698,955
2029	19,159,562	40,188,386	75,202,271
2030	19,653,105	40,686,816	75,705,588
2031	20,146,648	41,185,246	76,208,904
2032	20,640,191	41,683,675	76,712,220
2033	21,133,735	42,182,105	77,215,537
Total	147,377,449	306,124,929	570,428,009

The cost associated with the help desk is the opportunity cost for personnel in the General and Operations Manager occupation at covered entities

to call the help desk. CISA assumes that, on average, each covered entity that submits a report would call the help desk one time for each report submitted.

The number of help desk calls is based on the number of reports, although a help desk call could be for any aspect of CIRCIA compliance such as

⁴¹³ ICR 1670–0007 includes a burden of six hours per month to conduct electronic recordkeeping for CSAT. CISA applied the same six hours per month for CIRCIA, but only applies the burden to one month, as the covered entity is expected to undergo the recordkeeping burden only once, not on a recurring basis as with CSAT.

⁴¹⁴ Information on the hourly compensation rates used is contained in Section 3.2 of the Preliminary RIA. CISA requests comment on this cost, specifically on the level of burden required to

compile the data and the appropriate personnel to complete the task.

⁴¹⁵ The estimate of four terabytes is based on the average of all incident response activities that CISA Threat Hunting engaged in in FY 2022 and FY 2023, and includes incidents across Federal, SLTT, critical infrastructure and non-critical infrastructure private entities.

⁴¹⁶ Enterprise Storage Forum, *Cloud Storage Pricing in 2023: Everything You Need to Know*, available at <https://www.enterprisestorageforum.com/cloud/cloud-storage-pricing/>.

⁴¹⁷ CISA recognizes that the data retention period may be longer than two years, particularly for the estimated 50% of covered entities that submit one or more Supplemental Reports for a covered cyber incident. CISA assumes that covered entities currently retain data under normal business practices, and as such, only estimates the marginal cost of an additional two years over the current retention practices. CISA requests comment on this assumption.

registration, reporting, or data and record preservation. Based on similar costs for CSAT, CISA estimates an average time of ten minutes for a help desk call.⁴¹⁸ CISA estimates the cost per call by multiplying the time burden by the hourly compensation rate for the General and Operations Manager occupation of \$102.42. Multiplying this hourly compensation rate by ten minutes (0.17 hours) results in an average cost of a help desk call of \$17.07 for covered entities. Applying this cost

to the number of calls, CISA estimates the cost for help desk calls ranging from \$1.4 million to \$7.9 million, with a primary estimate of \$3.6 million.

The Preliminary RIA also details potential enforcement costs based on the opportunity cost for a covered entity to respond to a Request for Information or a subpoena issued by CISA, including costs associated with a potential appeal of a subpoena. CISA estimates a total 10-year enforcement cost of \$237,573, undiscounted. This is based on the

issuance of 100 RFIs, five subpoenas, and one appeal per year.

CISA estimates the undiscounted cost to industry could range from \$1.2 billion to \$3.2 billion, with a primary estimate of \$1.4 billion. Discounted at 2%, the primary cost would be \$1.3 billion, with an annualized cost of \$148.8 million. Table 8 presents the industry cost range for this analysis for the period from 2024 through 2033.

TABLE 8—INDUSTRY COST RANGE
[\$ Millions, undiscounted]

Year	Low estimate	Primary estimate	High estimate
2024	\$0.0	\$0.0	\$0.0
2025	467.0	467.0	1,171.6
2026	488.1	506.6	1,244.3
2027	37.6	65.6	114.5
2028	38.1	66.2	115.1
2029	38.7	66.7	115.7
2030	39.2	67.3	116.2
2031	39.8	67.8	116.8
2032	40.3	68.4	117.4
2033	40.9	69.0	117.9
Total	1,229.8	1,444.5	3,229.6

Note: Totals may not sum due to rounding.

Table 9 presents the primary industry cost estimate for the period of analysis.

TABLE 9—TOTAL INDUSTRY COST, PRIMARY ESTIMATE
[\$ Millions]

Year	Familiarization costs	Reporting costs	Data preservation costs	Help desk costs	Enforcement costs	Total	Discounted 2%
2024	\$0.0	\$0.0	\$0.0	\$0.00	\$0.00	\$0.0	\$0.0
2025	467.0	0.0	0.0	0.00	0.00	467.0	448.9
2026	475.1	9.7	21.3	0.44	0.03	506.6	477.3
2027	16.2	9.7	39.2	0.44	0.03	65.6	60.6
2028	16.2	9.8	39.7	0.44	0.03	66.2	59.9
2029	16.2	9.9	40.2	0.45	0.03	66.7	59.2
2030	16.2	9.9	40.7	0.45	0.03	67.3	58.6
2031	16.2	10.0	41.2	0.46	0.03	67.8	57.9
2032	16.2	10.0	41.7	0.46	0.03	68.4	57.2
2033	16.2	10.1	42.2	0.46	0.03	69.0	56.6
Total	1,055.5	79.1	306.1	3.59	0.24	1,444.5	1,336.2
Annualized							148.8

Note: Totals may not sum due to rounding.

Table 10 presents the total undiscounted industry cost by affected population.

⁴¹⁸ CISA, ICR 1670-0007 Supporting Statement A, uploaded May 23, 2019, available at https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=201905-1670-001. See Table 2, Estimated

Annual Burden Hours and Costs by Reporting by Instrument. CISA uses the previous ICR estimate of ten minutes for the help desk burden rather than the most recent estimate of seven minutes, since

CFATS is a more mature program and has been able to reduce help desk call times over time.

TABLE 10—COST BY COVERED ENTITY CRITERIA
[\$ Millions, undiscounted]

Affected population	Total 10-year cost, undiscounted
Not Covered Entities	\$432.0
Non-Small Entities	101.3
Owns or Operates a Covered Chemical Facility	9.4
Provides Wire or Radio Communications Service	205.3
Owns or Operates Critical Manufacturing Sector Infrastructure	123.1
Provides Operationally Critical Support to the Department of Defense or Processes, Stores, or Transmits Covered Defense Information	230.5
Performs an Emergency Service or Function	26.7
Bulk Electric and Distribution System Entities	12.1
Owns or Operates Financial Services Sector Infrastructure	123.8
Qualifies as a State, Local, Tribal, or Territorial Government Entity	9.3
Qualifies as an Education Facility	38.7
Entities Involved with Information and Communication Technologies Used to Support Core Election Processes	0.3
Provides Essential Public Health-Related Services	41.5
Information Technology Entities	19.3
Owns or Operators a Commercial Nuclear Power Reactor or Fuel Cycle Facility	0.3
Transportation System Entities	16.6
Subject to Regulation Under the Maritime Transportation Security Act	13.1
Owns or Operates a Qualifying Community Water System or Publicly Owned Treatment Works	41.2
Total	1,444.5

As discussed throughout Section 4 of the Preliminary RIA, there is a great deal of uncertainty in the cost estimates presented in this analysis. Because this would be a completely new regulatory program, it is difficult to predict precisely how the regulated population would respond. A number of assumptions used to estimate the costs have significant uncertainty around them, which has led CISA to develop a sensitivity analysis in the Preliminary RIA to account for this uncertainty. The main areas of uncertainty are:

- **Number of CIRCIA Report Submissions**—The number of reports is difficult to predict, as a mandatory reporting program with this scope does not currently exist, nor does a truly comparable program that CISA could use as a proxy. As such, CISA presents a range of possible outcomes for the number of reports submitted with percentages of entities reporting based on several data sources.

- **Time Burden for Familiarization**—Particularly as it relates to non-covered entities, CISA has no way to predict what level of effort such entities would invest in reading the rulemaking documents, nor can CISA predict the number of entities that would read all or some of the rulemaking documents, yet ultimately not be a covered entity. CISA also recognizes that there is a significant uncertainty regarding the time burden associated with a covered entity familiarizing themselves with the requirements. In this analysis, CISA estimates the cost based on the time

necessary to read the NPRM, which is expected to be similar to that of reading the Final Rule. There is additional uncertainty regarding the number of non-covered entities that would incur costs associated with familiarization. The current analysis estimates that approximately 12.9 million entities in critical infrastructure sectors would incur some costs associated with familiarization. However, it is unclear how many such entities would familiarize themselves with the rule, and whether or not entities outside critical infrastructure would potentially incur some familiarization costs to confirm that they are not covered entities (e.g., by reading the Applicability section and assessing whether they are or not in a critical infrastructure sector).

- **Means for Data and Records Preservation**—The analysis currently assumes that all covered entities that submit a report will comply with the Data and Records Preservation requirements by storing and maintaining digital records. CISA acknowledges that there may be some instances where hard copy records or data are maintained either in lieu of or in addition to at least some digital records, but does not estimate the potential cost of physical records. CISA expects that the cost of preserving physical records would replace, and be comparable to, the costs for digital records, rather be an additional cost of this provision.

- **Number of Enforcement Actions**—While CIRCIA empowers CISA to take enforcement action against covered entities that have not submitted required CIRCIA Reports, it is unclear how many of these actions CISA would take and which mechanisms would be leveraged. There is a great deal of uncertainty regarding how CISA would identify potentially non-compliant entities, as that would require CISA to be aware of an event that was not reported, or for CISA to be aware that an entity that reported has subsequently uncovered substantial new or different information than that which was previously reported. Until CISA operationalizes this program, it is unable to accurately predict the number or nature of enforcement actions that would be needed.

There may also be implementation costs to the government and cost savings to the affected population associated with CIRCIA’s substantially similar reporting exception, as discussed earlier in this NPRM. This reporting exception will allow covered entities subject to more than one Federal cyber incident reporting requirement to avoid having to report duplicative information to both CISA and another Federal agency when certain conditions are met. CISA believes that this exception would provide an overall cost savings, with the potential cost savings to the affected population through the avoidance of duplicative reporting requirements outweighing the implementation costs the government would incur (e.g., the

costs associated with drafting, negotiating, and entering into CIRCIA Agreements, as defined in § 226.1 of the proposed rule). Because CIRCIA Agreements cannot be fully developed, and this exception cannot be fully implemented, until the final rule stage or after implementation of the regulatory program, at this time, CISA is unable to estimate what the impact of this exception would be on either government costs or industry savings.⁴¹⁹

iii. Government Cost

CISA anticipates incurring significant costs associated with the creation, implementation, and operation of the government infrastructure to run the CIRCIA program. Implementing and operationalizing CIRCIA as statutorily mandated would require significant new government investment. This investment is necessary to develop and maintain the infrastructure, in both technology and personnel, necessary to receive, analyze, and share information from CIRCIA Reports submitted to CISA. While CISA exercised some discretion in the description of covered entities, this description was scoped in such a way that reducing the number of the entities subject to the rule in a manner that would materially impact the government cost (*i.e.*, by materially reducing the number of CIRCIA Reports received) would also sacrifice the extent to which the proposed rule would achieve the purpose of CIRCIA and the proposed rule, as described in section III.C.⁴²⁰ This is particularly true for the government costs, where much of the costs would be incurred regardless of the scope of covered entities (*e.g.*, the different aspects of the technology infrastructure). Further, as noted in section III.C, CISA believes that, due to advances in technology and strategies for managing large data sets, the potential challenges associated with receiving large volumes of reports can be mitigated through technological and procedural strategies.

CISA also has discretion in the period for Data and Records Preservation. However, this would not impact the

⁴¹⁹ While CISA does not estimate the cost for this provision, it is expected that the benefits to industry of avoiding duplicative reporting would exceed the costs to the government.

⁴²⁰ For more information on how CISA considered rescoping the description of covered entities, see Section 0 and Section 5 of the Preliminary RIA, which present alternative approaches to the description of covered entities.

government cost, as this is a cost borne by industry.

For fiscal year 2023, CISA budgeted \$34.5 million for CIRCIA related work. In 2024, CISA has requested \$97.7 million, to perform work necessary to prepare for CIRCIA implementation. This includes funding to support several efforts specifically mandated by CIRCIA or necessary for the practical implementation of the CIRCIA mandates, such as the rulemaking process; stakeholder outreach; and efforts to begin creating the technology infrastructure necessary to receive and share reports, report on and use the information collected under CIRCIA, and other key functions. Because funding requested for 2023 has already been allocated, this is considered part of the pre-regulatory baseline in the Preliminary RIA. Including the pre-regulatory baseline, CISA presents an 11-year government cost estimate for this proposed rule.⁴²¹

CISA anticipates needing an annual budget of approximately \$115.9 million to cover all the functions associated with CIRCIA. CISA anticipates this budget request to include funding for additional federal staff, contractor support, and new technology costs. Additional staffing would be necessary to conduct a myriad of mission-critical activities, such as analyzing the CIRCIA Reports to conduct trend and threat analysis, vulnerability and mitigation assessment, the provision of early warnings, incident response and mitigation, supporting Federal efforts to disrupt threat actors, and advancing cyber resiliency. Additional full-time equivalent staffing would be added to support the ingest of reports; engagement efforts, including a CIRCIA help desk;⁴²² CIRCIA enforcement actions; and other mission support roles. Technology costs would account for developing the infrastructure necessary to collect, maintain, automatically analyze, and share information from CIRCIA Reports as well as licenses, updates, and maintenance for CISA systems.⁴²³

⁴²¹ To account for the pre-regulatory baseline, CISA includes costs incurred in 2023. These costs are reverse discounted by applying the discount factor of 1.020 to the undiscounted cost of \$34.5 million in year 2023.

⁴²² CISA would need to provide a means for the regulated public to contact CISA for assistance with complying with the final regulation when it becomes effective.

⁴²³ Although CISA does not estimate industry costs for submitting CIRCIA reports until Year 3

As noted by the Cyberspace Solarium Commission, the government's cyber incident situational awareness, its ability to detect coordinated cyber campaigns, and its cyber risk identification and assessment efforts rely on comprehensive data and, prior to the passage of CIRCIA, the Federal government lacked a mandate to systematically collect cyber incident information reliably and at the scale necessary.⁴²⁴ The government investment discussed in the Preliminary RIA will provide CISA with the resources to meet the stated goals of CIRCIA. Specifically, the government cost presented in this NPRM will be used by CISA to develop and operationalize the system and infrastructure necessary to receive and analyze a sufficient quantity of Covered Cyber Incident Reports and Ransom Payment Reports from across critical infrastructure sectors, share information with stakeholders, and use that information and analysis to develop informational products and other tools to be shared with and leveraged by CISA's Federal and non-Federal stakeholders.

Because CISA has already begun making investments to operationalize the CIRCIA program in anticipation of the publication of the final rule in 2025, this analysis accounts for government costs from 2023 through 2033, or the full 10-year period of analysis and one year of pre-regulatory costs, even though industry would not incur costs until 2025 upon publication of the final rule. As presented in Table 11, CISA estimates an undiscounted government cost for CIRCIA of \$1.2 billion over the period of analysis from 2023 through 2033. Discounted at 2%, the government cost would be \$1.1 billion, with an annualized cost of \$108.1 million.

(2026), CISA anticipates requesting the full CIRCIA annual budget of \$115.9 million starting in Year 2 (2025) to ensure that all personnel and technology are in place once the Final Rule is published. As discussed below, there is a level of uncertainty regarding the government costs.

⁴²⁴ *Cyberspace Solarium Commission Report*, supra note 23, at 103; see also Sandra Schmitz-Berndt, "Defining the Reporting Threshold for a Cybersecurity Incident under the NIS Directive and the NIS 2 Directive," *Journal of Cybersecurity* at 2 (Apr. 5, 2023) ("[L]ow reporting levels result in a flawed picture of the threat landscape, which in turn may impact cybersecurity preparedness."), available at <https://academic.oup.com/cybersecurity/article/9/1/tyad009/7160387>.

TABLE 11—GOVERNMENT COST
[\$ Millions]

Year	Undiscounted	Discounted at 2%
2023	\$34.5	\$34.5
2024	97.7	95.8
2025	115.9	111.4
2026	115.9	109.2
2027	115.9	107.1
2028	115.9	105.0
2029	115.9	102.9
2030	115.9	100.9
2031	115.9	98.9
2032	115.9	97.0
2033	115.9	95.1
Total	1,175.3	1,057.7
Annualized		108.1

Note: Totals may not sum due to rounding.

iv. Combined Costs

Table 12 presents the combined industry and government costs over the period of analysis. Based on the primary estimates for industry’s costs presented

throughout Section 4 of the Preliminary RIA and the government costs presented in Section 5 of the Preliminary RIA, CISA estimates an undiscounted cost to industry and government over the

period of analysis of \$2.6 billion. Discounted at 2%, the estimated cost of this proposed rule over the period of analysis is \$2.4 billion, with an annualized cost of \$244.7 million.

TABLE 12—COMBINED INDUSTRY AND GOVERNMENT COST, PRIMARY ESTIMATE
[\$ Millions]

Year	Industry	Government	Total, undiscounted	Total, discounted 2%
2023	\$0.0	\$34.5	\$34.5	\$34.5
2024	0.0	97.7	97.7	95.8
2025	467.0	115.9	582.9	560.3
2026	506.6	115.9	622.5	586.6
2027	65.6	115.9	181.5	167.7
2028	66.2	115.9	182.1	164.9
2029	66.7	115.9	182.6	162.2
2030	67.3	115.9	183.2	159.5
2031	67.8	115.9	183.7	156.8
2032	68.4	115.9	184.3	154.2
2033	69.0	115.9	184.9	151.6
Total	1,444.5	1,175.3	2,619.8	2,394.0
Annualized				244.6

Note: Totals may not sum due to rounding.

Table 13 presents the cost range for combined industry and government costs, discounted at 2%. The costs over

the period of analysis range from a low estimate of \$2.2 billion to a high estimate of \$4.1 billion, and an

annualized range of \$225.4 million to \$415.4 million, discounted at 2%.⁴²⁵

TABLE 13—COMBINED INDUSTRY AND GOVERNMENT COST RANGE
[\$ Millions]

Year	Low estimate	Primary estimate	High estimate
2023	\$34.5	\$34.5	\$34.5
2024	95.8	95.8	95.8
2025	560.3	560.3	1,237.5
2026	569.1	586.6	1,281.8
2027	141.8	167.7	212.9
2028	139.5	164.9	209.2
2029	137.3	162.2	205.6
2030	135.1	159.5	202.1

⁴²⁵ This analysis uses 2023 as the base year for costs estimates.

TABLE 13—COMBINED INDUSTRY AND GOVERNMENT COST RANGE—Continued
[\$ Millions]

Year	Low estimate	Primary estimate	High estimate
2031	132.9	156.8	198.6
2032	130.7	154.2	195.2
2033	128.6	151.6	191.8
Total	2,205.6	2,394.0	4,065.1
Annualized	225.4	244.6	415.4

Note: Totals may not sum due to rounding.

v. Benefits

The primary purpose of CIRCIA is to help preserve national security, economic security, and public health and safety. The provisions included in this proposed rule would support that purpose in a number of ways, providing several benefits. In this analysis, CISA discusses the qualitative benefits of the proposed rule.

Over the last decade, the United States has seen an exponential increase in cyber incidents, with nation-states, criminal actors, and other malicious cyber threat actors targeting entities across all of the critical infrastructure sectors with ever-evolving tactics, techniques, and procedures. Addressing this growing, dynamic threat requires a better understanding of the threat and the vulnerabilities being exploited, and the timely sharing of that information with owners and operators of internet-connected information systems so that they can take steps to better secure themselves from potential cyber incidents. As noted by the Cyberspace Solarium Commission, “The government’s cyber incident situational awareness, its ability to detect coordinated cyber campaigns, and its risk identification and assessment efforts rely on comprehensive data. However, there are insufficient federal and state laws and policies requiring companies to report incidents that impact or threaten to impact business operations.”⁴²⁶ As discussed in greater detail below, CIRCIA would help the Federal government address this shortcoming by helping the Federal government understand the cyber threat landscape and enabling the timely sharing of information to enhance cyber resilience.

Under this proposed rule, covered entities would be required to report covered cyber incidents and ransom payments to CISA within the timeframes and other requirements described in the proposed rule. Collecting this information in a timely

fashion (within 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred or 24 hours after a ransom payment has been disbursed) would provide the Federal government with enhanced cross-sector visibility into the cyber threat landscape and support the aggregation, analysis, and sharing of incident data in a way that heretofore has been unavailable to the cybersecurity community. This, in turn, would facilitate a better understanding by both Federal and non-Federal entities of who is causing cyber incidents; what types of entities malicious cyber actors are targeting; what tactics, techniques, and procedures malicious cyber actors are using to compromise entities in critical infrastructure sectors; what vulnerabilities are being exploited; what security defenses are effective at stopping the incidents; and what mitigation measures are successful in reducing the consequences of an incident.

While not part of the proposed rule,⁴²⁷ CIRCIA recognizes the value of these activities and imposes upon CISA a number of requirements related to the analysis and sharing of information received through CIRCIA Reports to ensure their value is reasonably maximized. These obligations include:

- Aggregating and analyzing reports to assess the effectiveness of security controls; identify tactics, techniques, and procedures adversaries use to overcome these controls; assess potential impact of cyber incidents on public health and safety; and enhance situational awareness of cyber threats across critical infrastructure sectors;⁴²⁸
- Coordinating and sharing information with appropriate Federal departments and agencies to identify and track ransom payments;⁴²⁹
- Leveraging information gathered about cyber incidents to provide appropriate entities, including Sector

Coordinating Councils, Information Sharing and Analysis Organizations, SLTT governments, technology providers, cybersecurity and cyber incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures;⁴³⁰

- For significant cyber incidents, reviewing the details surrounding the incident or group of incidents and identifying and disseminating ways to prevent or mitigate similar cyber incidents in the future;⁴³¹
- Publishing quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations;⁴³²
- Proactively identifying opportunities to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations;⁴³³ and
- Making information received in CIRCIA Reports available to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.⁴³⁴

By requiring CISA to perform these analytical activities and share information and analytical the findings with Federal and non-Federal stakeholders—an obligation CISA intends to fulfill through a variety of information sharing mechanisms, including through the development, maintenance, and issuance of publicly available alerts, advisories, a known exploited vulnerabilities catalog, and other products that can be leveraged by both covered entities and non-covered entities—CIRCIA will indirectly enhance the nation’s overall level of cybersecurity and resiliency, resulting in direct, tangible benefits to the nation. For example:

⁴³⁰ 6 U.S.C. 681a(a)(3)(B).
⁴³¹ 6 U.S.C. 681a(a)(6).
⁴³² 6 U.S.C. 681a(a)(8).
⁴³³ 6 U.S.C. 681a(a)(9).
⁴³⁴ 6 U.S.C. 681a(a)(10).

⁴²⁶ *Cyberspace Solarium Commission Report*, supra note 23, at 103–04.

⁴²⁷ As Congress imposed these obligations solely on Federal departments and agencies, they are not included in the CIRCIA proposed rule itself.

⁴²⁸ 6 U.S.C. 681a(a)(1).

⁴²⁹ 6 U.S.C. 681a(a)(2).

- By supporting CISA's ability to share information that will enable non-Federal and Federal partners to detect and counter sophisticated cyber campaigns earlier with the potential for significant avoided or mitigated negative impacts to critical infrastructure or national security, CIRCIA's mandatory reporting requirements reduce the risks associated with those campaigns.⁴³⁵

- By facilitating the identification and sharing of information on exploited vulnerabilities and measures that can be taken to address those vulnerabilities, incident reporting enables entities with unremediated and unmitigated vulnerabilities on their systems to take steps to remedy those vulnerabilities before the entity also falls victim to cyberattack.⁴³⁶

- By supporting sharing information about common threat actor tactics, techniques, and procedures with the IT community, cyber incident reporting will enable software developers and vendors to develop more secure products or send out updates to add security to existing products, better protecting end users.⁴³⁷

⁴³⁵ See, e.g., *Stakeholder Perspectives Hearing*, *supra* note 17, at 17–18 (statement of FireEye Mandiant Vice President Ronald Bushar) (“Timely reporting of incidents within and across sectors allow[s] for earlier detection of large, sophisticated cyber campaigns that have the potential for significant impacts to critical infrastructure or National security implications. Technical indicators, along with contextual information, provide a more robust data set to conduct faster and more accurate attribution in adversary intent. This type of analysis is critical in formulating the most impactful response to such attacks and to do so in a time frame that has a high probability of successful countermeasures or deterrence.”). See also Mandiant, *Analysis of Time-to-Exploit Trends: 2021–2022* (Sept. 28, 2023), available at <https://www.mandiant.com/resources/blog/time-to-exploit-trends-2021-2022>.

⁴³⁶ See, e.g., *Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack: Hearing Before the Subcomms. on Cybersecurity, Infrastructure Protection, and Innovation & Transportation and Maritime Security of the H. Comm. on Homeland Security*, 117th Cong. 21 (June 15, 2021) (testimony of CISA Cybersecurity Division Executive Assistant Director Eric Goldstein) (“With increased visibility, we are able to better identify adversary activity across sectors, which allows us to produce more targeted guidance. . . .”), available at <https://www.congress.gov/event/117th-congress/joint-event/LC69050/text> (hereinafter “*CHS June 15, 2021 Hearing*”); Bitsight Security Research, *A Mere Five Percent of Vulnerable Enterprises Fix Their Issues Every Month: How to Help Them Do Better?* (May 3, 2023), available at <https://www.bitsight.com/blog/mere-five-percent-vulnerable-enterprises-fix-their-issues-every-month-how-help-them-do-better> (noting that CISA alerts and advisories can increase the likelihood of rapid cybersecurity vulnerability remediation by nearly five times the likelihood of rapid remediation for cybersecurity vulnerabilities for which there is no CISA alert or advisory).

⁴³⁷ See, e.g., *Open Hearing: Hack of U.S. Networks by a Foreign Adversary Before the S. Select Comm. on Intelligence*, 117th Cong. (Feb. 23,

- By enabling rapid identification of ongoing incidents and increased understanding of successful mitigation measures, incident reporting increases the ability of impacted entities and the Federal government to respond to ongoing campaigns faster and mitigate the consequences that could result from them.⁴³⁸

- Law enforcement entities can use the information submitted in reports to investigate, identify, capture, and prosecute perpetrators of cybercrime, getting malicious cyber actors off the street and deterring future actors.⁴³⁹

- By contributing to a more accurate and comprehensive understanding of the cyber threat environment, incident reporting allows for CISA's Federal and non-Federal stakeholders to more efficiently and effectively allocate resources to prevent, deter, defend against, respond to, and mitigate significant cyber incidents.⁴⁴⁰ Please

2021) (written testimony of SolarWinds CEO Sudhakar Ramakrishna) (“Indicators of compromise associated with [cybersecurity] events shared with software vendors in an anonymized way enriches the understanding of prevailing threat actor techniques and target sets, enabling software providers to improve defenses and better protect users.”), available at <https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary>.

⁴³⁸ See, e.g., *id.* (written testimony of Microsoft President Brad Smith) (“A private sector disclosure obligation will foster greater visibility, which can in turn strengthen a national coordination strategy with the private sector which can increase responsiveness and agility.”); *Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective: Hearing Before the S. Comm. on Homeland Security and Governmental Affairs*, 117th Cong. (Mar. 18, 2021) (opening statement of Sen. Gary Peters, Chairman) (“In order to adapt to the evolving cybersecurity threat, both the public and private sector need a centralized, transparent, and streamlined process for sharing information. In the event of a future attack[,], this will be critical to mitigating the damage.”), available at <https://www.hsgac.senate.gov/hearings/understanding-and-responding-to-the-solarwinds-supply-chain-attack-the-federal-perspective/> (hereinafter “*HSGAC March 18, 2021 Hearing*”).

⁴³⁹ See, e.g., *HSGAC March 18, 2021 Hearing*, *supra* note 438 (statement of FBI Cyber Division Acting Assistant Director Tonya Ugoretz) (“[The SolarWinds attack] highlighted how vital private sector cooperation is to our broader work protecting America from cyber threats. The virtuous cycle we can drive when we work together has been on display in the SolarWinds response: information from the private sector fuels our investigations, allows us to identify evidence and adversary infrastructure, and enables us to hand off leads to intelligence and law enforcement partners here and abroad. Our partners then put that information to work and hand us back more than we started with, which we can then use to arm the private sector to harden itself against the threat. By leaning into our partnerships, all of us who are combating malicious cyber activity become stronger while we weaken the perpetrators together.”).

⁴⁴⁰ See, e.g., *CHS June 15, 2021 Hearing*, *supra* note 436, at 15 (statement of TSA Assistant Administrator for Surface Operations Sonya Proctor) (“By requiring the reporting of cybersecurity incidents, the Federal Government is

also see the discussion of market failure associated with the current patchwork system of cyber incident reporting that exists today and why a centralized regulatory system to collect incident reports is needed to correct this failure, in Section 1.2 of the Preliminary RIA.

Even before CIRCIA, one of the core mechanisms through which CISA achieves its cybersecurity mission is producing and widely sharing timely and actionable operational alerts and advisories on known threats, incidents, and vulnerabilities. The broad sharing of timely information enables CISA to make an impact at scale and buy down broad swaths of risk. CISA leverages many information sharing mechanisms and partnership communities to ensure that relevant information is reaching the targeted audience.⁴⁴¹ There are many ways in which CISA ensures that alerts, advisories, analysis, and specific vulnerability or threat information is widely shared to the broadest appropriate audience, including:

- Working to prioritize stakeholder awareness of actively exploited vulnerabilities through maintenance of a known exploited vulnerability (KEV) catalog which is available on CISA's website. Members of the public can also subscribe to the GovDelivery notification subscription to receive email notifications whenever the KEV catalog is updated.

- Leveraging several communities to ensure broadest appropriate dissemination of guidance to specific communities of interest, such as through Sector Risk Management Agencies, Information Sharing & Analysis Centers (ISACs), and CISA regional personnel to engage state and local governments, critical infrastructure, and other communities directly.

- Depending on the severity of the threat, vulnerability, or threat actor campaign, CISA may reach out directly to potentially impacted entities to try to ensure their awareness and recommended mitigations, if available.

better positioned to understand the changing threat of cyber events and the current and evolving risks to pipelines.”); *Stakeholder Perspectives Hearing*, *supra* note 17, at 20 (statement of FireEye Mandiant Vice President Ronald Bushar) (“[R]obust and centralized collection of incident information provides the Government with a much more accurate cyber risk picture and enables more effective and efficient investments and support before, during, and after major cyber attacks.”).

⁴⁴¹ CISA shares and disseminates information in myriad ways, including via the *CISA.gov* website and/or the *StopRansomware.gov* website, various social media platforms, and the GovDelivery email notification subscription. Information is also shared with the Homeland Security Information Network (HSIN), U.S. Cyber Centers, and through direct stakeholder engagement.

- CISA shares cyber threat indicators, based on information shared with CISA by CISA partners or generated through CISA's own analysis and engagements, via the Automated Indicator Sharing platform.

- Working with other federal and industry partners, as appropriate, who will also disseminate alerts/advisories through their information sharing mechanisms.

Through CIRCIA reporting, CISA would be able to gather more time-sensitive threat and vulnerability data regarding covered cyber incidents or ransomware attacks. This timely collection of specific data elements, fed into CISA's existing robust communication channels, described above, would allow for sharing of a higher volume of actionable information that is more timely and could be used to reduce risk and mitigate against losses associated with covered cyber incidents and ransom payments. The reporting of covered cyber incidents by impacted entities would provide information that could reduce the number of incidents with consequences through increased awareness of attack vectors and vulnerabilities, leading to more informed covered entities (and non-covered entities) taking preventative or protective measures based on the shared information. This would allow entities to either reduce the losses associated with incidents for which they have been a victim, or for entities to take protective measures prevent an incident altogether. Through early identification and warning of threat actor tactics, cyber incidents, or vulnerabilities, CISA would be able to help entities recognize potential weaknesses and implement protective measures to prevent cyber incidents or limit the consequences of cyber incidents.

By creating a centralized regulatory incident reporting system, CIRCIA can help the Federal government develop a comprehensive understanding of known incidents and ransom payments. Under the current patchwork reporting system, many incidents go unreported, other incidents are reported with limited technical information that results in limited ability to use the reports to help prevent other incidents, and there is no reliable mechanism to ensure that reports are being shared broadly enough across the Federal government or between the Federal government and non-Federal partners to make the reported information actionable to mitigate against negative impacts. A robust, rich, and consolidated incident reporting program, facilitated by the proposed rule, would make the

realization of the benefits listed above far more likely, comprehensive, useful, and timely.

These benefits, which stem from the reporting of cyber incidents for aggregation, analysis, and information sharing, directly contribute to a reduction in economic, health, safety, and security consequences associated with cyber incidents by reducing the likelihood of cyber incidents successfully perpetrated and mitigating the consequences of those cyber incidents that are successful by catching them earlier. For example, incident reporting to CISA within 72 hours and CISA's sharing of that information has a number of benefits associated with rapid vulnerability remediation. For example: (1) vendors that receive earlier warning of previously undisclosed vulnerabilities can begin to develop patches sooner, reducing the likelihood of an incident resulting from their exploitation; (2) entities that remediate a vulnerability rapidly can reduce the likelihood of a known vulnerability being exploited by reducing the period of time during which their systems are vulnerable to exploitation of that vulnerability; (3) entities that remediate a vulnerability rapidly can reduce the likelihood of the propagation of a threat within their systems, which would reduce the impact of a vulnerability that has already been exploited (*i.e.*, reducing the severity of an incident); and (4) awareness that a vulnerability is being actively exploited by threat actors can help entities effectively prioritize their remediation and patching efforts (as entities often have more patches in the queue than their personnel can realistically remediate in a timely fashion). In an analysis of its proprietary dataset of cyber claims, the Marsh McLennan Cyber Risk Analytics Center compared cyber controls in terms of their effectiveness in reducing the likelihood of an organization experiencing a cyber event. Although patching was identified as one of the most effective controls, tied for fourth, it was found to have one of the lowest implementation rates.⁴⁴² However, a recent study suggests that information put out by CISA is meaningfully shaping how entities are implementing this highly effective control. Bitsight Security Research found that CISA alerts and advisories can increase the likelihood of rapid cybersecurity vulnerability remediation by nearly five

⁴⁴² Marsh McLennan, *Using data to prioritize cybersecurity investments* (2023), available at <https://www.marsh.com/us/services/cyber-risk/insights/using-cybersecurity-analytics-to-prioritize-cybersecurity-investments.html>.

times the likelihood of rapid remediation for vulnerabilities for which there is no CISA alert or advisory, outpacing the impact of even sustained social media coverage:

Further, strategic coverage of vulnerabilities in CISA briefings (Alerts and Current Activity advisories) can accelerate the pace of their remediation, boosting the probability of rapid remediation by around 4.7x. Even greater impacts may be possible, which would be highly desirable. Sustained coverage of vulnerabilities on social media, *e.g.* Twitter, is associated with boosting their prospects of rapid remediation by roughly 2.7x.⁴⁴³

By identifying a vulnerability through CIRCIA reporting, and disseminating that information quickly and broadly, CISA can provide earlier disclosure to vendors of zero-day vulnerabilities and early warning to potentially impacted entities to take preventative or protective measures to remediate known vulnerabilities before they become exploited.⁴⁴⁴ CISA requests comment on the potential impact of reporting requirements for preventing or mitigating cybersecurity incidents.

It is worth noting that these benefits are not limited to covered entities required to report under CIRCIA, but also inure to entities not subject to CIRCIA's reporting requirements as they too will receive the downstream benefits of enhanced information sharing, more secure technology products, and an ability to better defend their networks based on sector-specific and cross-sector understandings of the threat landscape.

CISA also anticipates qualitative benefits stemming from the data and record preservation requirements of this proposed rule. The preservation of data and records in the aftermath of a covered cyber incident serves a number of critical purposes, such as supporting the ability of analysts and investigators to understand how a cyber incident was perpetrated and by whom. Access to forensic data, such as records and logs, can help analysts uncover how malicious cyber activity was conducted, what vulnerabilities were exploited, what tactics were used, and so on. This information can be essential to preventing others from falling victim to similar incidents in the future. How an incident was perpetrated may not be immediately identifiable upon

⁴⁴³ Bitsight Security Research, *A Mere Five Percent of Vulnerable Enterprises Fix Their Issues Every Month: How to Help Them Do Better?* (May 3, 2023), available at <https://www.bitsight.com/blog/mere-five-percent-vulnerable-enterprises-fix-their-issues-every-month-how-help-them-do-better>.

⁴⁴⁴ See also Mandiant, *Analysis of Time-to-Exploit Trends: 2021–2022* (Sept. 28, 2023), available at <https://www.mandiant.com/resources/blog/time-to-exploit-trends-2021-2022>.

discovery of an incident, and the failure to properly preserve data or records during the period of initial incident response can render it difficult to subsequently perform this analysis. This can especially be true in incidents involving zero-day vulnerabilities or highly complex malicious cyber activity by nation state threat actors, such as the “SUNBURST” malware that compromised legitimate updates of customers using SolarWinds products or the Hafnium campaign on Exchange servers, with the full extent, cause, or attribution of an incident often not being known until months after the initial discovery.⁴⁴⁵

In designing the proposed rule, CISA sought the approach that would provide the best balance between qualitative benefits and the costs associated with implementation of the rule. For instance, in determining the proposed scope of the covered entity population, CISA attempted to balance the need for sufficient reporting necessary to achieve the benefits described in this section with the recognition that the larger the covered entity population, the greater the costs associated with the rule would be.⁴⁴⁶ In light of that, as described in Section IV.B, CISA worked closely with its Federal partners to carefully target specific types of entities from each critical infrastructure sector for inclusion after consideration of the three factors enumerated in 6 U.S.C. 681b(c)(1) and the entities’ ability to manage the reporting requirements. Based on that, CISA is proposing to cover only a small portion of the millions of entities “in a critical infrastructure sector” that could have been included in the description of covered entities.

Another example of where CISA looked to maximize qualitative benefits relative to costs is in the content that a covered entity is required to submit when making a Covered Cyber Incident Report. CISA generally focused on requiring content that was either specifically enumerated as required content in the CIRCIA legislation or that CISA believes is necessary for CISA to accomplish an obligation imposed upon CISA by the legislation.

Similarly, as described in Section IV.F, regarding data preservation, CISA felt that there are significant benefits from requiring entities to retain data for an extended period of time. When determining the data preservation

timeframe, CISA considered existing best practices regarding preservation of information related to cyber incidents, data retention or preservation requirements from comparable regulatory programs, and comments received on this issue from stakeholders in response to the CIRCIA RFI and at CIRCIA listening sessions. Based on the above, CISA believes that a data preservation requirement lasting anywhere between two and three years would be consistent with existing best practices, would be implementable by the regulated community, and would achieve the purposes for which data preservation is intended under CIRCIA. Recognizing that the costs for preserving data increase the longer the data must be retained, and wanting to limit costs of compliance with CIRCIA where possible without sacrificing the ability to achieve the intended purposes, CISA is proposing a length at the lower end of the spectrum of best practices for data preservation. While many regulatory regimes require data to be preserved for three years or more, CISA has elected to propose a two-year reporting period. CISA believes the two-year period would provide the best balance between qualitative benefits and costs by balancing the incremental costs of continued data retention against the benefits of having incident data available for an extended period of time following an incident.

In addition to identifying the qualitative benefits discussed above, CISA considered a break-even analysis. Break-even analysis is useful when it is not possible to quantify the benefits of a regulatory action. OMB Circular A–4 recommends a “threshold” or “break-even” analysis when non-quantified benefits are important to evaluating the benefits of a regulation. Threshold or break-even analysis answers the question, “How small could the value of the non-quantified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?”⁴⁴⁷ OMB Circular A–4 notes that “It may be useful to focus a break even analysis on whether the action under consideration will change the probability of events occurring or the potential magnitude of those events. For example, there may be instances when you have estimates of the expected outcome of a type of catastrophic event, but assessing the change in the probability of such an event may be difficult. Your break-even analysis could demonstrate how much a

regulatory alternative would need to reduce the probability of a catastrophic event occurring in order to yield positive net benefits or change which regulatory alternative is most net beneficial.”⁴⁴⁸

In the past, DHS has used a break-even analysis to compare the costs of a proposed rule to the expected impacts of a terrorist attack, or other extremely rare, high consequence event. This analysis would differ for CIRCIA, as this proposed rule would help prevent or mitigate far more common cybersecurity incidents that, as discussed in Section 1.1 of the Preliminary RIA, occur more often, and with an increased frequency since 2018.

Agencies typically use break-even to produce a conditional justification for the proposed rule. While this conditional justification does not resolve whether or not a rule would break-even, or reach net-zero benefits, it serves to highlight what information is missing and what kind of assumptions would be necessary to provide a basis for the proposed rule to break-even.⁴⁴⁹ According to Sunstein, break-even analysis helps agencies “. . . to specify the source of uncertainty, and what they would need to know in order to reduce it. Conditional justifications have the advantage of transparency, because they specify the factual assumptions that would have to be made for the benefits to justify the costs. That specification is exceedingly important, because it can promote accountability, promote consideration of the plausibility of the underlying assumptions, and promote testing and revisiting over time as new information becomes available.”⁴⁵⁰

CISA expects this proposed rule to reduce the risk of loss of critical services or financial losses due to a covered cyber incident in the critical infrastructure sectors. As described above, upon receiving a Covered Cyber Incident Report or Ransom Payment Report, the statute requires CISA to undertake a number of analytical and information-sharing efforts. The development and sharing of actionable information about cyber threats, security vulnerabilities, and defensive measures can help other entities to avoid the costs of a cyber incident in two ways.

First, the information would allow some entities to take actions that prevent the incident from occurring. For example, this could lead to discovery of a zero-day vulnerability earlier in time,

⁴⁴⁵ See, e.g., *Evidence Preservation*, *supra* note 370.

⁴⁴⁶ See Section III.C.ii for a discussion of why a sufficient number of reports is needed to achieve the purposes of CIRCIA.

⁴⁴⁷ OMB, Circular A–4 (Sept. 17, 2003), available at https://obamawhitehouse.archives.gov/omb/circulars_a004_a-4/.

⁴⁴⁸ *Id.*

⁴⁴⁹ Cass R. Sunstein, “The Limits of Quantification,” 102 *California Law Review* 102, no. 6 (2014).

⁴⁵⁰ *Id.*

resulting in earlier vendor development and customer deployment of a patch; recognition that a previously identified vulnerability is one being actively exploited by threat actors, resulting in its remediation being prioritized;⁴⁵¹ or identification of a new threat actor tactic, technique, or procedure, for which companies can deploy enhanced network or end-point scanning and blocking.

Second, even where an incident is not prevented, the information would allow other entities to mitigate the impacts of the incident (e.g., by reducing the propagation of the incident throughout the organization). Incidents occur in different stages (often referred to as the “lifecycle” of a cyber incident); the earlier in the lifecycle a network defender can identify an incident, the more likely network defenders can negate or impede the adversary from

achieving their goals.⁴⁵² This means that earlier detection of incidents minimizes both the impact to systems and data (and the associated damage from that impact) and the cost of containment, remediation, and recovery.

CISA requests comment on the potential use of a break-even analysis in this case, specifically on what the consequences of a substantial cyber incident would be, and the number of substantial cyber incidents expected in a given year. Additionally, CISA requests comment on how effective early notification of cyber incidents would be in mitigating expected consequences of an incident.

When thinking about benefits, CISA considered estimates of the cost of a covered cyber incident from the Information Risk Insights Study (IRIS) 2022 by the Cyentia Institute, which was sponsored by CISA. The Cyentia Institute analyzed Advisen’s Cyber Loss

Data, which is widely used and presents the most comprehensive list of historical cyber incidents. From the July 2022 Advisen dataset, the Cyentia Institute analyzed the 1,893 cyber events with reported loss data, from the 10-year period ranging from 2012 to 2021. These predominately U.S. events impacted firms across all 20 NAICS sectors at the two-digit level and were assigned to one of eight patterns: Denial of Service Attack, Accidental Disclosure, Scam or Fraud, System Intrusion, Insider Misuse, Physical Threats, Ransomware, and System Failure. Of these eight pattern types, System Intrusion was found to be both the most frequent (49.6% of all types) and to have the highest financial impact (60.2% of the total impact across all types). Table 14 presents summary statistics associated with these 1,893 cyber events.⁴⁵³

TABLE 14—SUMMARY OF CYBER EVENT LOSSES AND COUNTS, IRIS 2022

Measure	Loss	Number of events (2012–2021) ^a	Average annual number of events
Minimum	\$32	0	0
First Quartile	29,000	474	47.4
Geometric Mean	266,000	479	47.9
Third Quartile	2,000,000	458	45.8
95th Percentile	52,000,000	386	38.6
Maximum	12,000,000,000	96	9.6

Note. Data is based on data from the Cyentia Institute’s IRIS 2022 study.

^a These are the number of events that resulted in losses between the breakpoints of each of the following loss bin: [\$0, \$32), [\$32, \$29,000), [\$29,000, \$266,000), [\$266,000, \$ 2 million), [\$2 million, \$52 million), and [\$52 million, \$12 billion]. Since the minimum value of \$32 is the single lowest loss that occurred among the 1,893 events, there are no events associated with it in this column. Instead, there are 474 events which had losses from \$32 up to \$29,000, 479 events from \$29,000 up to \$266,000, and so on.

As noted in the Cyentia Institute IRIS 2022 report, the typical cost of a security incident is close to the geometric mean of \$266,000, and the average, or arithmetic mean, is over \$25 million. Rather than require reporting of any cyber incident, this rule proposes to require reporting only of covered cyber incidents, which means a substantial cyber incident experienced by a covered entity. Under the proposed rule, a substantial cyber incident means a Cyber Incident that leads to any of the following:

1. Substantial loss of confidentiality, integrity, or availability;
2. Serious impact on safety and resiliency of operational systems and processes;

3. Disruption of ability to engage in business or industrial operations, or deliver goods or services; or

4. Unauthorized access facilitated through or caused by a: (1) compromise of a cloud service provider, managed service provider, or other third-party data hosting provider, or (2) supply chain compromise.⁴⁵⁴

Although none of these impacts is defined in terms of event loss, in its report “IRIS 20/20 Xtreme,” Cyentia Institute describes losses associated with business interruptions, which are included in the third type of impact for substantial cyber events.⁴⁵⁵ Cyentia Institute finds that business interruptions are the most numerous event category, with over half of all total losses attributable to business

interruption, and have high median losses of \$82 million. Because this rule proposes to require incident reporting only for covered cyber incidents, which must by definition be substantial cyber incidents, CISA considered comparing the cost of this proposed rule to the 95th percentile loss value of \$52 million, which is closer to the estimate of \$82 million and perhaps more representative of what a substantial cyber incident may cost. CISA again welcomes comment on the potential application of these and other estimates.

vi. Accounting Statement

The OMB A–4 Accounting Statement (Table 15) presents annualized costs and qualitative benefits of the proposed rule in 2022 dollars.

⁴⁵¹ CISA, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, <https://www.cisa.gov/known-exploited-vulnerabilities> (last visited Nov. 28, 2023).

⁴⁵² See, e.g., MITRE, *Overview of How Cyber Resiliency Affects the Cyber Attack Lifecycle* (2015),

available at <http://www2.mitre.org/public/industry-perspective/documents/lifecycle-ex.pdf>.

⁴⁵³ Cyentia Institute, *Information Risk Insights Study 2022*, tbl. 3, Loss Summary, available at <https://www.cyentia.com/iris-2022/>.

⁴⁵⁴ See § 226.1 of the proposed rule.

⁴⁵⁵ Cyentia Institute, *Information Risk Insights Study IRIS 20/20 Xtreme* (2020), tbl. 4, Event Top Level Category, available at <https://www.cyentia.com/wp-content/uploads/IRIS2020-Xtreme.pdf>.

TABLE 15—OMB A-4 ACCOUNTING STATEMENT
[\$ Millions, 2022 dollars]

Category	Estimates			Units			Notes
	Primary estimate	Low estimate	High estimate	Year dollar	Discount rate (%)	Period covered (years)	
Cost Savings							
Quantitative Annualized Monetized (\$ millions/year).	N/A	N/A	N/A	N/A	2	N/A	
Qualitative	Qualitative benefits include (a) improved incident reporting and response and (b) improved cybersecurity posture through improved ability to prevent or mitigate events through information sharing, early warning, threat analysis, and incident response. The preservation of data and records in the aftermath of a covered cyber incident serves a number of critical purposes, such as supporting the ability of (a) analysts and investigators to understand how a cyber incident was perpetrated and by whom and (b) law enforcement to capture and prosecute perpetrators of cyber incidents and recover ill-gotten proceeds from the criminal activity						
Costs							
Annualized Monetized (\$ millions/year)	\$244.6	\$225.4	\$415.4	2023	2	10	NPRM RIA.
Transfers							
From/To	From: N/A			To: N/A			
Other Annualized Monetized (\$ millions/year)	N/A	N/A	N/A	N/A	2	N/A	
From/To	From:	N/A		To:	N/A		
Effects							
State, Local, and/or Tribal Government—Annualized Monetized (\$ millions/year).	\$10.1				2	10	NPRM RIA (Section 11.2.1). IRFA (Section 9).
Small Business	Conducted Initial Regulatory Flexibility Analysis (IRFA).						
Wages	None						
Growth	Not measured						

vii. Alternatives

As part of this analysis, CISA considered alternatives to the proposed rule. Below, CISA presents the four alternatives considered for this rulemaking along with the estimated costs. When comparing alternatives, CISA reviewed the cost of each alternative as well as the objective of the rulemaking effort and the benefits associated with each alternative. While CISA did not estimate quantitative benefits for each alternative, the qualitative benefits for each alternative provide context as to why the NPRM alternative is the preferred choice for CISA.

1. The Preferred Alternative—The NPRM

The analysis for this alternative was discussed above, as it is the proposed alternative. As presented in Section V.A.iv, CISA estimates a combined industry and government cost of \$2.6 billion over the period of analysis, and an annualized cost of \$244.6 million, discounted at 2%.

CISA selected this alternative as the preferred alternative, as it would provide the best balance between qualitative benefits and costs while

being responsive to the statutorily mandated requirements of CIRCIA. While there are potential lower cost alternatives, the scoping of the population of covered entities in the preferred alternative allows CISA to capture adequate reporting populations from not just the sector-based criteria, but also from entities in multiple critical infrastructure sectors and subsectors using a single threshold.

As discussed above in Section IV.B.iv.1, there are several benefits to including the size-based criterion in the population of covered entities. CISA believes that substantial cyber incidents at larger entities routinely will have a higher likelihood of disrupting the reliable operation of critical infrastructure, making timely knowledge by CISA of any covered cyber incidents affecting larger entities in critical infrastructure sectors essential for potential mitigation of negative consequences. Also, larger entities are more likely to identify early signs of compromise than smaller entities because larger entities also are likely to have more mature cybersecurity capabilities or be better situated to bring in outside experts to

assist during an incident.⁴⁵⁶ By including large entities in the description of covered entity, the likelihood that an incident is noticed and reported is increased, while the timeframe between initiation of an incident and its reporting is likely to be decreased, making any potential mitigation efforts more effective. CISA also believes that large entities would be better situated to simultaneously report and respond to or mitigate an incident. Because large entities represent a disproportionate percent of the impacts of covered cyber incidents on critical infrastructure, are more likely to be able to identify a cover cyber incident earlier, and respond more quickly while mitigating an incident, CISA believes that the inclusion of the size-based criterion will materially improve the content and volume of reports that CISA receives.

Additionally, the data and record preservation requirements put forth in the preferred alternative are consistent with existing best practices, help ensure the ability to assess and analyze an incident as new information comes to light related to this specific incident or type of incident, support eventual

⁴⁵⁶ Verizon 2022 DBIR, supra note 181, at 65.

attribution of an incident that may not be known in the immediate aftermath of the incident, and increase the likelihood that necessary data and records are preserved long enough to support investigation and prosecution of the threat actors responsible for carrying out the incident. Any reduction in these provisions, while reducing burden, would not justify the sacrifice in benefits. In the following sections for each alternative, CISA more fully explains why each proposed alternative was rejected.

2. Alternative 1—Reduce the Data and Record Preservation Period

For this alternative, CISA reduces the proposed data and record preservation period from two years to six months. A six-month period would align with existing FBI Letters of Preservation, which allow for an initial 90-day duration, with the option to request preservation for another 90-day period, if needed. Under this alternative, there would be no change to the CIRCIA reporting requirements and therefore, no changes to the costs estimated for becoming familiar with the rule,

reporting, help desk, or enforcement of CIRCIA.

Under this alternative, we estimate the costs only for six months of storage, which is the equivalent of multiplying the number of reports per year by \$500, without accounting for storage costs after the year the report was submitted.

Table 16 presents the industry cost for Alternative 1 (based on the primary estimates presented in Section V.A.ii), which CISA estimated would be \$1.2 billion over the period of analysis and \$129.2 million annualized at a 2% discount rate.

TABLE 16—ALTERNATIVE 1 INDUSTRY COST, PRIMARY ESTIMATE
[\$ Millions]

Year	Familiarization costs	Reporting costs	Data & record preservation costs	Help desk costs	Enforcement costs	Total	
						Undiscounted	Discounted 2%
2024	\$0.0	\$0.0	\$0.0	\$0.00	\$0.00	\$0.0	\$0.0
2025	467.0	0.0	0.0	0.00	0.00	467.0	448.9
2026	475.1	9.7	12.5	0.44	0.03	497.8	469.1
2027	16.2	9.7	12.7	0.44	0.03	39.1	36.1
2028	16.2	9.8	12.8	0.44	0.03	39.3	35.6
2029	16.2	9.9	13.0	0.45	0.03	39.5	35.1
2030	16.2	9.9	13.2	0.45	0.03	39.7	34.6
2031	16.2	10.0	13.3	0.46	0.03	40.0	34.1
2032	16.2	10.0	13.5	0.46	0.03	40.2	33.6
2033	16.2	10.1	13.6	0.46	0.03	40.4	33.2
Total	1,055.5	79.1	104.6	3.59	0.24	1,243.0	1,160.2
Annualized							129.2

Note: Totals may not sum due to rounding.

Under this alternative, CISA would not anticipate a change in Federal government costs, which would remain \$1.2 billion, discounted at 2%, over the

period of analysis for government costs (see Table 11). The combined costs for industry and government under Alternative 1 are presented in Table 17.

CISA estimates a combined 11-year cost of \$2.2 billion and an annualized cost of \$226.7 million, discounted at 2%.

TABLE 17—ALTERNATIVE 1 COMBINED INDUSTRY AND GOVERNMENT COST, PRIMARY ESTIMATE
[\$ Millions]

Year	Industry cost	Government cost	Total cost	
			Undiscounted	Discounted 2%
2023	\$0.0	\$34.5	\$34.5	\$34.5
2024	0.0	97.7	97.7	95.8
2025	467.0	115.9	582.9	560.3
2026	497.8	115.9	613.7	578.3
2027	39.1	115.9	155.0	143.2
2028	39.3	115.9	155.2	140.6
2029	39.5	115.9	155.4	138.0
2030	39.7	115.9	155.6	135.5
2031	40.0	115.9	155.9	133.0
2032	40.2	115.9	156.1	130.6
2033	40.4	115.9	156.3	128.2
Total	1,243.0	1,175.3	2,418.3	2,218.0
Annualized				226.6

Note: Totals may not sum due to rounding.

Alternative 1 represents a cost savings compared to the Preferred Alternative of \$176.0 million over the period of

analysis, all of which is realized due to the reduction of the data and record preservation period. While Alternative 1

would implement CIRCIA at a lower cost than the Preferred Alternative, CISA rejects this alternative because it

would not convey the full benefits associated with the data and record preservation requirements. The data and record preservation requirements can support the ability of analysts and investigators to understand how a cyber incident was perpetrated and by whom as well as enable data and trend analysis and the investigation of incidents. This could lead to a reduction or mitigation of the risk of future cyber incidents.

The reduction in the data and record preservation requirements would weaken the ability for CISA and other agencies to assess and analyze an incident as new information that may come to light related to this specific incident or type of incident, support eventual attribution of an incident that may not be known in the immediate aftermath of the incident. Reducing the data and records preservation period would also decrease the likelihood that necessary data and records are preserved long enough to support investigation and prosecution of the

threat actors responsible for carrying out the incident. Any reduction in these provisions, while reducing burden, would not justify the sacrifice in benefits.

3. Alternative 2—Remove Size-Based Criterion

For this alternative, CISA would decrease the affected population of covered entities by removing the size-based criterion for covered entities. This change would reduce the population of covered entities by 35,152 (see Section 8.3 of the Preliminary RIA) to 284,607 covered entities, which would be approximately a 12% reduction from the Preferred Alternative. Although this alternative estimates the cost savings for the removal of all 35,152 covered entities identified under the size-based criterion, it is unlikely that the removal of this criterion would result in the removal of all covered entities in the size-based criterion. CISA, however, does not have an estimate for the

number of covered entities that would be removed from the affected population of covered entities based on the removal of the size-based standard. As discussed in Section IV.B.iv, CISA recognizes that additional sector-based criteria would be developed in lieu of the size-based standard, however, CISA has not yet developed the thresholds that would be necessary to define these additional criteria. For this alternative, CISA conducted the analysis using the same methodology as presented in the Preferred Alternative.

Table 18 presents the industry cost for Alternative 2. CISA estimated all costs using the methodology for obtaining the primary estimates presented in Section V.A.ii above and Section 4 of the Preliminary RIA, but based on the reduced population of covered entities. CISA estimated the total cost to industry would be \$1.1 billion over the period of analysis and \$119.7 million annualized at a 2% discount rate.

TABLE 18—ALTERNATIVE 2 INDUSTRY COST, PRIMARY ESTIMATE
[\$ Millions]

Year	Familiarization	Reporting costs	Data & record preservation costs	Help desk costs	Enforcement costs	Total	Discounted 2%
2024	\$0.0	\$0.0	\$0.0	\$0.0	\$0.0	\$0.0	\$0.0
2025	395.3	0.0	0.0	0.0	0.0	395.3	380.0
2026	401.0	7.0	9.2	0.3	0.0	417.6	393.5
2027	11.5	7.0	29.0	0.3	0.0	47.9	44.2
2028	11.5	7.1	29.5	0.3	0.0	48.4	43.9
2029	11.5	7.2	30.0	0.3	0.0	49.0	43.5
2030	11.5	7.2	30.5	0.3	0.0	49.5	43.1
2031	11.5	7.3	31.0	0.3	0.0	50.1	42.8
2032	11.5	7.3	31.5	0.3	0.0	50.7	42.4
2033	11.5	7.5	32.0	0.3	0.0	51.3	42.1
Total	876.6	50.2	190.6	2.3	0.21	1,159.8	1,075.4
Annualized							119.7

Under this alternative, CISA would not anticipate a change in Federal government costs, which would remain \$1.2 billion over the 11-year period of analysis for government costs. CISA assumes no change in government cost due to the relatively small impact

associated with the removal of the size-based criterion. Additionally, since government costs are based on expected budget requests, there is a high degree of uncertainty regarding how this change would impact that request. The combined costs for industry and

government under Alternative 2 are presented in Table 19. CISA estimates a combined 11-year cost of \$2.1 billion and an annualized cost of \$218.0 million, discounted at 2%.

TABLE 19—ALTERNATIVE 2 COMBINED INDUSTRY AND GOVERNMENT COST, PRIMARY ESTIMATE
[\$ Millions]

Year	Industry cost	Government cost	Total cost	
			Undiscounted	Discounted 2%
2023	0.0	34.5	34.5	34.5
2024	0.0	97.7	97.7	95.8
2025	395.3	115.9	511.2	491.4
2026	417.6	115.9	533.5	502.7
2027	47.9	115.9	163.8	151.3
2028	48.4	115.9	164.3	148.8
2029	49.0	115.9	164.9	146.4

TABLE 19—ALTERNATIVE 2 COMBINED INDUSTRY AND GOVERNMENT COST, PRIMARY ESTIMATE—Continued
[\$ Millions]

Year	Industry cost	Government cost	Total cost	
			Undiscounted	Discounted 2%
2030	49.5	115.9	165.4	144.0
2031	50.1	115.9	166.0	141.7
2032	50.7	115.9	166.6	139.4
2033	51.3	115.9	167.2	137.2
Total	1,159.8	1,175.3	2,335.1	2,133.1
Annualized				218.0

While Alternative 2 would present a lower cost than the Preferred Alternative, there are several reasons why it was rejected in favor of the Preferred Alternative. As discussed in Section IV.B, there are a wide variety of types of entities that are active participants in critical infrastructure sectors and communities and are considered “in a critical infrastructure sector.” Rather than develop sector-based criteria for each of these potential categories of covered entities, CISA relies on the size-based criterion to capture entities in these sectors and subsectors that are not otherwise covered in the sector-based criteria and for which CISA considered that requiring reporting only from large entities was sufficient to meet CIRCIA’s purposes. Including these entities is critical for the following reasons, as described in further detail in section IV.B.iv.1:

- While size is not alone indicative of criticality, larger entities’ larger customer bases, market shares, number of employees, and other similar size-based characteristics mean that cyber incidents affecting them typically have greater potential to result in consequences impacting national security, economic security, or public health and safety than cyber incidents affecting smaller companies.
- Large entities disproportionately experience cyber incidents.
- Non-small entities are likely to own or operate a disproportionate percentage of the nation’s critical infrastructure.
- In light of the interconnectedness of the world today, incidents at entities in critical infrastructure sectors that are not themselves owners and operators of critical infrastructure can have cascading effects that end up impacting critical infrastructure. Based on this, CISA believes that substantial cyber incidents at larger entities routinely will

have a high likelihood of disrupting the reliable operation of critical infrastructure.

Removing the size-based criterion would limit CISA’s ability to collect valuable information from a broader set of entities than relying on the sector-based criteria would allow. Furthermore, removing the size-based criterion would require CISA to develop additional sector-based criteria to capture entities from certain critical sectors or subsectors, such as Food and Agriculture Sector entities, Commercial Facilities, Oil and Natural Gas Subsector entities, and medical laboratories that currently are included in the description of covered entity primarily or solely based on the size-based criterion. Covering these additional entities is much more in line with the purpose of the regulation for CISA to learn about new or novel vulnerabilities, trends, or tactics sooner and be able to share early warnings before additional entities within the sector, critical or non-critical, can fall victim to them.

Contrary to the minimum benefits (in terms of industry cost savings) likely to be gained by elimination of the size-based criterion, CISA believes there are significant reasons to include the criterion in the proposal. First, as described at length in Section IV.B.iv.1, there are a number of reasons why CISA believes requiring reporting from large entities is beneficial. This includes the belief that substantial cyber incidents at larger entities routinely will have a high likelihood of disrupting the reliable operation of critical infrastructure, making timely knowledge by CISA of any covered cyber incidents affecting larger entities in critical infrastructure sectors essential for potential mitigation of negative consequences; larger entities are more likely to identify early signs of compromise than smaller entities; large entities would be better situated to

simultaneously report and respond to or mitigate an incident; and the inclusion of the size-based criterion will materially improve the content and volume of reports that CISA receives. Second, the size-based criterion allows CISA to capture adequate reporting from multiple sectors and subsectors using a single threshold. As noted above, without the size-based criterion, CISA likely would need to establish one or more new sector-based criteria for each of at least five critical infrastructure sectors or subsectors, and has included alternative proposed sector-based criteria in the proposed rulemaking for this purpose. In total, while CISA believes it could achieve the purposes of the CIRCIA statute without a size-based criterion, CISA believes that the benefits of including the size-based criterion far exceed the almost certainly minimal cost savings associated with an alternative where additional sector-based criteria are used in lieu of the size-based criterion.

4. Alternative 3—Reduce the Data and Record Preservation Requirement and Remove Size-Based Criterion

For this alternative, CISA would combine the cost reductions presented in Alternative 1 and Alternative 2 to present the lowest cost alternative.

Table 20 presents the industry cost for Alternative 3. CISA estimated all costs, with the exception of the data and record preservation costs, using the methodology for obtaining the primary estimates presented in Section V.A.ii. CISA estimated the data and records preservation costs using the same methodology used under Alternative 1 as presented in Section V.A.vii.a. CISA estimated the total cost to industry would be \$950.0 million over the period of analysis and \$105.7 million annualized at a 2% discount rate.

TABLE 20—ALTERNATIVE 3 INDUSTRY COST, PRIMARY ESTIMATE
[\$ Millions]

Year	Familiarization costs	Reporting costs	Data & record preservation costs	Help desk costs	Enforcement costs	Total	
						Undiscounted	Discounted 2%
2024	\$0.0	\$0.0	\$0.0	\$0.0	\$0.00	\$0.0	\$0.0
2025	395.3	0.0	0.0	0.0	0.00	395.3	380.0
2026	401.0	7.0	9.2	0.3	0.03	417.6	393.5
2027	11.5	7.0	9.4	0.3	0.03	28.3	26.1
2028	11.5	7.1	9.6	0.3	0.03	28.5	25.8
2029	11.5	7.2	9.7	0.3	0.03	28.7	25.5
2030	11.5	7.2	9.9	0.3	0.03	28.9	25.2
2031	11.5	7.3	10.0	0.3	0.03	29.2	24.9
2032	11.5	7.3	10.2	0.3	0.03	29.4	24.6
2033	11.5	7.5	10.4	0.3	0.03	29.7	24.4
Total	876.6	57.7	78.4	2.7	0.24	1,015.5	949.9
Annualized						105.7	

Note: Totals may not sum due to rounding.

Under this alternative, CISA would not anticipate a change in Federal government costs, which would remain \$1.2 billion over the 11-year period of

analysis for government costs. The combined costs for industry and government under Alternative 3 are presented in Table 21. CISA estimates a

11-year cost of \$2.0 billion and an annualized cost of \$205.1 million, discounted at 2%.

TABLE 21—ALTERNATIVE 3 COMBINED INDUSTRY AND GOVERNMENT COST, PRIMARY ESTIMATE
[\$ Millions]

Year	Industry cost	Government cost	Total cost	
			Undiscounted	Discounted 2%
2023	\$0.0	\$34.5	\$34.5	\$34.5
2024	0.0	97.7	97.7	95.8
2025	395.3	115.9	511.2	491.4
2026	417.6	115.9	533.5	502.7
2027	28.3	115.9	144.2	133.2
2028	28.5	115.9	144.4	130.8
2029	28.7	115.9	144.6	128.4
2030	28.9	115.9	144.8	126.1
2031	29.2	115.9	145.1	123.8
2032	29.4	115.9	145.3	121.6
2033	29.7	115.9	145.6	119.4
Total	1,015.5	1,175.3	2,190.8	2,007.6
Annualized				205.1

Note: Totals may not sum due to rounding.

Alternative 3 estimates the lowest cost alternative in this analysis, which presents a lower burden based on changes to discretionary elements in two required provisions—a reduction in the data and records preservation requirements and a reduction in the number of covered entities through the removal of the size-based criterion. As discussed in Sections V.A.vii.b and c, the reduction in the data preservation period and the removal of the size-based criterion, while reducing costs, would sacrifice benefits as compared to Preferred Alternative.

5. Alternative 4—Increase the Affected Population to All Critical Infrastructure Entities

For this alternative, CISA widened the description of covered entity to include all entities operating in the 16 critical infrastructure sectors.⁴⁵⁷ Under this alternative, the affected population would increase from 316,244 covered entities to 13,180,483 covered entities. This population was estimated by using the manner of determining whether an entity is in a critical infrastructure

sector as explained in Section IV.B.ii. As discussed above, the SSPs for each critical infrastructure sector include a sector profile of entities in the sector.⁴⁵⁸ The number of covered entities within each sector, was based on information in the SSPs, as well as populations based on NAICS codes for the affected industries, which was estimated using U.S. Census County Business Patterns data. Table 22 presents the affected population for each of the 16 critical infrastructure sectors. This affected population would include small and not

⁴⁵⁷ The 16 critical infrastructure sectors listed by Presidential Policy Directive 21. See <https://obama.whitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/> (last visited Nov. 28, 2023).

⁴⁵⁸ The list of 16 Critical Infrastructure Sectors can be found at <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors> (last visited Nov. 28, 2023).

small businesses, based on SBA size standards, within the 16 critical infrastructure sectors. standards, within the 16 critical infrastructure sectors.

TABLE 22—AFFECTED POPULATION BY CRITICAL INFRASTRUCTURE SECTOR

Criteria	Affected population	Percentage of affected population		
		2%	5%	10%
Chemical Sector	31,717	634	1,586	3,172
Commercial Facilities Sector	7,980,640	159,613	399,032	798,064
Communications Sector	92,861	1,857	4,643	9,286
Critical Manufacturing Sector	46,259	925	2,313	4,626
Dams Sector	107,054	2,141	5,353	10,705
Defense Industrial Base Sector	60,000	1,200	3,000	6,000
Emergency Services	118,098	2,362	5,905	11,810
Energy Sector	36,069	721	1,803	3,607
Financial Services Sector	294,794	5,896	14,740	29,479
Food and Agriculture Sector	3,239,083	64,782	161,954	323,908
Government Facilities Sector	89,626	1,793	4,481	8,963
Healthcare and Public Health Sector	142,806	2,856	7,140	14,281
Information Technology Sector	557,000	11,140	27,850	55,700
Nuclear Reactors, Materials, and Waste Sector	143	3	7	14
Transportation Systems Sector	214,833	4,297	10,742	21,483
Water and Wastewater Sector	169,500	3,390	8,475	16,950
Total	13,180,483	263,610	659,024	1,318,048

Using all of the same assumptions for the primary estimates presented in Sections V.A.i and ii, this would increase the number of expected CIRCIA Reports from 210,525 to 5,292,818 over the period of analysis. This would significantly increase the cost to industry, which is estimated to be \$31.8 billion over the period of analysis, or \$3.5 billion annualized, discounted at 2%, as presented in Table 23.

TABLE 23—ALTERNATIVE 4 INDUSTRY COST, PRIMARY ESTIMATE
[\$ Millions]

Year	Familiarization costs	Reporting costs	Data & record preservation costs	Help desk costs	Enforcement costs	Total cost	
						Undiscounted	Discounted 2%
2024	\$0.0	\$0.0	\$0.0	\$0.0	\$0.00	\$0.0	\$0.0
2025	10,461.9	0.0	0.0	0.0	0.00	10,461.9	10,055.7
2026	10,799.4	384.3	235.6	11.3	0.03	11,430.6	10,771.3
2027	675.0	384.4	732.8	11.3	0.03	1,803.5	1,666.1
2028	675.0	384.4	733.3	11.3	0.03	1,804.0	1,634.0
2029	675.0	384.5	733.8	11.3	0.03	1,804.6	1,602.4
2030	675.0	384.5	734.3	11.3	0.03	1,805.1	1,571.5
2031	675.0	384.6	734.8	11.3	0.03	1,805.7	1,541.1
2032	675.0	384.7	735.3	11.3	0.03	1,806.3	1,511.4
2033	675.0	384.8	735.8	11.3	0.03	1,806.9	1,482.3
Total	25,986.1	3,076.2	5,375.8	90.3	0.24	34,528.6	31,835.8
Annualized							3,544.2

Note: Totals may not sum due to rounding.

In addition to increased industry cost, CISA assumes that the substantial increase in volume of CIRCIA Reports submitted would lead to increased Federal government costs necessary to manage a much larger CIRCIA program. For the purposes of this alternatives analysis, CISA assumes a 10X (900%) increase in government cost in response to the 4,967% increase in the affected population. As presented in Table 24, CISA estimates a combined 11-year cost of \$42.1 billion, with an annualized cost of \$4.3 billion, discounted at 2%, for Alternative 4.

TABLE 24—ALTERNATIVE 4 COMBINED INDUSTRY AND GOVERNMENT COSTS, PRIMARY ESTIMATE
[\$ Millions]

Year	Industry cost	Government cost	Total cost	
			Undiscounted	Discounted 2%
2023	\$0.0	\$34.5	\$34.5	\$34.5
2024	0.0	977.0	977.0	957.8

TABLE 24—ALTERNATIVE 4 COMBINED INDUSTRY AND GOVERNMENT COSTS, PRIMARY ESTIMATE—Continued
[\$ Millions]

Year	Industry cost	Government cost	Total cost	
			Undiscounted	Discounted 2%
2025	10,461.9	1,159.0	11,620.9	11,169.7
2026	11,430.6	1,159.0	12,589.6	11,863.5
2027	1,803.5	1,159.0	2,962.5	2,736.8
2028	1,804.0	1,159.0	2,963.0	2,683.7
2029	1,804.6	1,159.0	2,963.6	2,631.6
2030	1,805.1	1,159.0	2,964.1	2,580.5
2031	1,805.7	1,159.0	2,964.7	2,530.3
2032	1,806.3	1,159.0	2,965.3	2,481.2
2033	1,806.9	1,159.0	2,965.9	2,433.1
Total	34,528.6	11,442.5	45,971.1	42,102.7
Annualized				4,302.0

Note: Totals may not sum due to rounding.

While Alternative 4 would capture a significantly larger affected population, and therefore provide CISA with additional data to use in its efforts to prevent, or mitigate the impact of, covered cyber incidents, this alternative is rejected due to its high cost. CISA would not anticipate additional benefits comparable to the cost increase from

expanding the population, as the Preferred Alternative focuses the affected population on the highest-risk population within the critical infrastructure sectors and is expected to provide sufficient reporting for CISA to identify cyber incident threats and trends.

6. Alternative Comparison

In this analysis, CISA considered four regulatory alternatives to the Preferred Alternative. Table 25 presents the cost comparison for the Preferred Alternative and the four additional alternatives discussed.

TABLE 25—ALTERNATIVES SUMMARY, COMBINED INDUSTRY AND GOVERNMENT COST, PRIMARY ESTIMATE
[\$ Millions]

Alternative	Description	11-Year cost		Annualized cost
		Undiscounted	Discounted 2%	Discounted 2%
Preferred	Proposed Rulemaking	\$2,619.8	\$2,394.0	\$244.6
1	Reduces the data and record preservation period	2,418.3	2,218.0	226.6
2	Remove Size Based Criterion for Covered Entities ⁴⁵⁹	2,335.1	2,133.1	218.0
3	Reduces the data and record preservation period and removes the size-based criterion.	2,190.8	2,007.6	205.1
4	Increases the affected population to all critical infrastructure entities	45,971.1	42,102.7	4,302.0

⁴⁵⁹ In this proposed rule, CISA proposes several criteria in § 226.2 to describe entities that would be considered covered entities, and one criterion would include entities that exceed the SBA small business size standard. Alternatives 2 and 3 would remove that as a criterion for determining covered entities.

B. Small Entities

The Regulatory Flexibility Act (RFA), 5 U.S.C. 603, requires agencies to consider the impacts of its rules on small entities. In accordance with the RFA, CISA has prepared an initial regulatory flexibility analysis (IRFA) that examines the impacts of the proposed rule on small entities. The IRFA is included in the Preliminary RIA that is available in the docket for this rulemaking. The term “small entities” comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of fewer than 50,000.

CISA is publishing the IRFA in the rulemaking docket to aid the public in commenting on the potential small

entity impacts of the requirements in this proposed rule. CISA invites all interested parties to submit data and information regarding the potential economic impact on small entities that would result from the adoption of the proposed requirements in this proposed rule. Under section 603(b) and (c) of the RFA, an IRFA must describe the impact of the proposed rule on small entities and contain the following:

- A description of the reasons why action by the agency is being considered.
- A succinct statement of the objectives of, and legal basis for, the proposed rule.
- A description of and, where feasible, an estimate of the number of small entities to which the proposed rule would apply.

- A description of the projected reporting, recordkeeping, and other compliance requirements of the proposed rule, including an estimate of the classes of small entities which would be subject to the requirements and the type of professional skills necessary for preparation of the report or record.

- An identification, to the extent practicable, of all relevant Federal rules which may duplicate, overlap, or conflict with the proposed rule.
- A description of any significant alternatives to the proposed rule that accomplish the stated objectives of applicable statutes and may minimize any significant economic impact of the proposed rule on small entities.

CISA has discussed many of these issues in other sections of the preamble

to the NPRM and in the Preliminary RIA, which is published in the rulemaking docket. CISA welcomes comment from the public on the Preliminary RIA.

An estimated 316,244 covered entities would be subject to requirements proposed in this NPRM and potentially incur costs as a result of this proposed rule. These covered entities include businesses, government entities, and organizations—some of which are considered to be small entities as defined by the RFA.

CISA does not have a complete list of the entities that would be subject to the requirements of this proposed rule. Therefore, as discussed in Section 9.4 of the Preliminary RIA, CISA conducted an analysis to review the NAICS codes that would most likely have entities affected by the proposed rule. Using the SBA size standards, CISA estimated the number of small entities within each of the 280 relevant NAICS codes. CISA then performed an IRFA to assess the impacts on small entities resulting from this proposed rule using the estimated cost per covered entity.

Based on the IRFA, CISA found:

- Of the 316,244 covered entities, CISA estimates that 310,855 would be considered small entities.
- Of the 264 NAICS codes with available revenue data, 99.2% had a revenue impact of less than or equal to 1%.
- CISA estimated that the average cost per non-covered entity would be \$33.58 and the average cost per covered entity experiencing a single covered cyber incident would be \$4,139.60.

CISA has discussed many of these issues in other sections of the NPRM and in the Preliminary RIA, which is published in the rulemaking docket. CISA welcomes comment from the public on the Preliminary RIA and the IRFA.

C. Assistance for Small Entities

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104–121), CISA wants to assist small entities in understanding this proposed rule so that they can better evaluate its effects on them and participate in the rulemaking. If this proposed rule would affect your small business, organization, or governmental jurisdiction and you have questions concerning its provisions or options for compliance, please contact the person in the **FOR FURTHER INFORMATION CONTACT** section of this NPRM. CISA will not retaliate against small entities that question or complain about this proposed rule or any policy or action of the CISA.

D. Collection of Information

Under the Paperwork Reduction Act of 1995 (PRA), 44 U.S.C. 3501–3520, agencies are required to submit to OMB, for review and approval, any reporting requirements inherent in a rule. This proposed rule would call for a new collection of information under PRA. CIRCIA also includes a broad exemption to PRA, which provides that: “Sections 3506(c), 3507, 3508, and 3509 of title 44 shall not apply to any action to carry out this section.” 6 U.S.C. 681b(f). CISA interprets the phrase “this section” as referring to 6 U.S.C. 681b for the purposes of the PRA exemption. Therefore, CISA understands the scope of this PRA exemption as applying to all information collection related to CIRCIA’s reporting requirements under 6 U.S.C. 681b(a)(1)–(3) as wholly exempt from compliance with the PRA, regardless of whether that information must be required under this proposed rule or is voluntarily provided in response to an optional question in a CIRCIA Report.

Covered entities will also have the opportunity to submit additional data and information to enhance situational awareness of cyber threats, as authorized under 6 U.S.C. 681c(b), via an open text box and/or the ability to upload information as part of a covered entity’s CIRCIA Report. Because CISA does not plan to require covered entities to submit this data and information, nor will it pose identical questions that must be responded to in any particular form or time period to covered entities, this additional information does not constitute a “collection of information” under the Paperwork Reduction Act. See 5 CFR 1320.3(c).

Accordingly, information collected through CIRCIA Reports, including additional information collected in an ad hoc manner that is incorporated into CIRCIA Reports, is exempt from compliance with PRA requirements. Information collected by CISA entirely pursuant to 6 U.S.C. 681c is outside of the scope of this rulemaking and not exempt from compliance with PRA requirements.

E. Federalism

Under Executive Order 13132, Federalism, 64 FR 43255 (Aug. 10, 1999), agencies must adhere to fundamental federalism principles, policymaking criteria, and in some cases follow additional requirements when promulgating federal regulations. While it is possible that the regulations proposed through this notice may have some impact on SLTT governments, CISA believes that this rule would not

trigger the additional requirements contained in Executive Order 13132 for rules that have federalism impacts.

Depending on the type of rule under development, Executive Order 13132 may require an agency to: (1) provide the State and local government with funds to pay for the direct costs they incur in complying with the regulation; (2) consult with State and local officials early in the process of developing the proposed regulation; (3) provide a federalism summary impact statement in the preamble of the rule; and/or (4) provide the Director of OMB with written communications submitted to the agency by State and local officials. Under Section 6 of the Executive Order, agencies must meet these additional requirements for two categories of rules. Section 6(b) describes the first category as rules that have federalism implications, impose substantial direct compliance costs on State and local governments, and that are not required by statute. Because the regulations proposed through this notice are required by statute, this proposed rule is not the sort of action contemplated by Section 6(b). The second category, described in Section 6(c) is a rule that would have federalism implications and that would preempt state law. While the regulations proposed through this notice may have some impact on SLTT governments, the rule would not have federalism implications as defined in Executive Order 13132, nor would the majority of this rule preempt state law.

A rule has implications for federalism under Executive Order 13132 if it has a substantial direct effect on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. While this proposed rule describes covered entity to include State and local government entities and entities like emergency service or education providers that may be considered part of a State, the requirement to file a CIRCIA Report is not a substantial direct effect under Executive Order 13132. Congress explicitly prohibited CISA from pursuing enforcement against a State or local government for failure to report a covered cyber incident or ransom payment as otherwise required under the statute’s implementing regulations. See 6 U.S.C. 681d(f). Thus, even though these proposed regulations require some State and local governments and government entities to report covered cyber incidents and ransom payments to CISA, this requirement is unenforceable. CISA believes that an unenforceable requirement to submit an informational

report to a federal agency is not the type of government action that results in a substantial direct effect on States, the relationship between the States and the national government, or the distribution of power or responsibilities among the various levels of government. Accordingly, CISA believes that this proposed rule would not have sufficient federalism implications that require under Executive Order 13132 preparation of a federalism summary impact statement, nor require further consultation with State and local government officials.

Similarly, the majority of this rule would not preempt State and/or local government law. Congress did not include any express preemption provision in the CIRCIA statute, and CISA does not assert through this rulemaking that the Federal government so fully occupies the field of cyber incident reporting that States or local governments cannot also regulate in this space. To CISA's knowledge, no State or local laws directly conflict with the incident reporting requirements set forth by this regulation, but CISA welcomes comment from stakeholders explaining otherwise.

One exception to this general lack of preemption is the set of statutory provisions included in CIRCIA, replicated in the proposed rulemaking for clarity in § 226.18(a)(5)(A) and (b)(2), that places limits on a State and/or local government's ability to use information obtained solely through a CIRCIA Report, and disclose the CIRCIA Reports themselves. Similar to the restriction placed on federal regulatory use of information obtained through reporting to CISA under CIRCIA, CIRCIA prohibits SLTT governments from using information about a covered cyber incident or ransom payment obtained solely through reporting directly to CISA under CIRCIA to regulate the activities of the covered entity or entity that made the ransom payment, unless the SLTT expressly permitted the entity to submit a CIRCIA Report to comply with its SLTT reporting obligations. See 6 U.S.C. 681e(a)(5).⁴⁶⁰ Similarly, in addition to exemption from disclosure under the Federal FOIA, CIRCIA also exempts CIRCIA Reports from disclosure under SLTT freedom of information laws or similar laws requiring disclosure of information or records. See U.S.C. 681e(b)(3). CISA believes, however, that incorporation of

these provisions into the proposed rule does not result in a rule that implicates federalism as contemplated under Executive Order 13132 for several reasons. First, these two information protection provisions, are a small, supportive aspect of the CIRCIA regulations and will only actually be implicated if and when SLTT governments receive CIRCIA Reports, or information included therein. Unless the SLTT government is in possession of a CIRCIA Report or information obtained solely through a CIRCIA Report after it has been submitted to CISA, these restrictions do not apply. Further, regarding the regulatory use restrictions, SLTT governments are not prohibited from taking regulatory actions based on information they receive from another source, even if that very same information was submitted to CISA as part of a CIRCIA Report. Congress prohibited from using the information obtained *solely* through a CIRCIA Report for such regulatory purposes, unless the submission of a CIRCIA Report is expressly permitted to meet SLTT reporting requirements. In other words, the rule would only place limits on SLTT governments' use and disclosure of information that they would not have otherwise obtained (and therefore, as a practical matter, would not have had in their possession to use or disclose) but for the rule itself. Second, these provisions are expected to inure to the benefit of SLTT governments by making it possible for CIRCIA Reports and/or information contained in those reports that is provided to the Federal government to be shared with the States, which CISA would not otherwise be able to do without risking the important confidentiality and other stakeholder protections required by CIRCIA. This ultimately means that SLTT governments will have more information (e.g., to protect their own information systems) than they would have had without the rule. Accordingly, CISA does not believe that this rule contains federalism implications and preempts state law in the manner that would trigger additional steps required for certain regulatory actions under Executive Order 13121.

Although CISA believes that Executive Order 13132 does not require adherence to the additional steps otherwise necessary for rules that have federalism implications and which preempt state law, CISA notes that representatives from several State and local government entities were consulted early in the development of this proposed rule. CISA hosted several

listening sessions between September and November 2022 to obtain input from those entities who may be impacted by the proposed regulations once they have been finalized. Representatives from various State and local government entities were invited to and attended these listening sessions. In some cases, representatives from State and local entities provided input on the proposed regulations during the listening session, for example, during the Emergency Services Sector and Government Facilities Sector sector-specific listening sessions. Transcripts of those listening sessions are available in the docket for this rulemaking.

CISA welcomes public comments on Executive Order 13132 federalism implications.

F. Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act of 1995 or UMRA, 2 U.S.C. 1531–1538, directs Federal agencies to assess the effects of regulatory actions on State, local, and tribal governments, and the private sector. UMRA's requirements apply when any Federal mandate may result in the expenditure by a State, local, or tribal government, in the aggregate, or by the private sector of \$100,000,000 (which is now \$177,000,000 when adjusted for inflation) or more in any one year.⁴⁶¹ This proposed rule does not impose an unfunded Federal mandate on State, local, or tribal governments because the proposed reporting requirements are unenforceable against SLTT Government Entities.⁴⁶² Although this proposed rulemaking would not impose an unfunded mandate on State, local, or tribal governments, the estimates for years 2 and 3 show an unfunded mandate in excess of \$177 million on the private sector primarily due to the estimated familiarization costs with the final rule. The regulatory impact assessment prepared in conjunction with this proposed rule satisfies

⁴⁶¹ \$100 million in 1995 dollars adjusted for inflation to 2022 using the GDP implicit price deflator for the U.S. economy. Federal Reserve Bank of St. Louis, "GDP Implicit Price Deflator in United States," available at <https://fred.stlouisfed.org/series/USAGDPDEFSAISME#0>, last accessed on July 21, 2023.

⁴⁶² See Memorandum for the Heads of Executive Departments and Agencies, *Guidance for Implementing Title II of S. 1*, from Alice Rivlin, OMB Director (Mar. 31, 1995) ("As a general matter, a Federal mandate includes Federal regulations that impose enforceable duties on State, local, and tribal governments, or on the private sector . . ."), available at https://obamawhitehouse.archives.gov/omb/memoranda_1998 (last accessed Oct. 13, 2023). See also 5 U.S.C. 1555 which defines a federal mandate as ". . . any provision in statute or regulation or any Federal court ruling that imposes an enforceable duty upon State, local, or tribal governments . . ." (emphasis added).

⁴⁶⁰ A CIRCIA Report may, consistent with State regulatory authority specifically relating to the prevention and mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such systems. 6 U.S.C. 681e(a)(5)(B).

UMRA's requirements under 2 U.S.C. 1532.

G. Taking of Private Property

This proposed rule would not cause a taking of private property or otherwise have taking implications under Executive Order 12630, Governmental Actions and Interference with Constitutionally Protected Property Rights, 53 FR 8863 (Mar. 18, 1988).

H. Civil Justice Reform

This proposed rule meets the applicable standards set forth in section 3(a) and 3(b)(2) of Executive Order 12988, Civil Justice Reform, 61 FR 4729 (Feb. 5, 1996) to minimize litigation, eliminate ambiguity, and reduce burden.

I. Protection of Children

This proposed rule, while "economically significant" under Executive Order 12866 as amended by Executive Order 14094, does not concern an environmental health risk or safety risk that an agency has reason to believe may disproportionately affect children. Accordingly, no further analysis is needed under Executive Order 13045, Protection of Children from Environmental Health Risks and Safety Risks, 62 FR 19885 (Apr. 21, 1997).

J. Indian Tribal Governments

This rule does not have "tribal implications" under Executive Order 13175, Consultation and Coordination With Indian Tribal Governments, 65 FR 67249 (Nov. 6, 2000), because it does not have substantial direct effects on one or more Indian tribes, on the relationship between the Federal government and Indian tribes, or on the distribution of power and responsibilities between the Federal government and Indian tribes. As with State and local governments, this proposed rule describes "covered entity," to include tribal government entities and entities like emergency service providers that may be considered part of a tribal government. The requirement to file a CIRCIA Report, however, is not a substantial direct effect under Executive Order 13175. Further, Congress explicitly prohibited CISA from pursuing enforcement against a tribal government for failure to report a covered cyber incident or ransom payment as otherwise required under the statute's implementing regulations. See 6 U.S.C. 681d(f). Accordingly, CISA believes that this rule does not have tribal implications, and therefore Executive Order 13175 requires no further agency

action or analysis. CISA welcomes public comments on Executive Order 13175 tribal implications.

K. Energy Effects

CISA has analyzed this proposed rule under Executive Order 13211, Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution, or Use, 66 FR 28355 (May 18, 2001). CISA has determined that it is not a "significant energy action" under that order because even though it is a "significant regulatory action" under Executive Order 12866, it is not likely to have a significant adverse effect on the supply, distribution, or use of energy, and it has not been designated by the Administrator of the Office of Information and Regulatory Affairs as a "significant energy action." Accordingly, the provisions of Executive Order 13211 to not apply to this proposed rule.

L. Technical Standards

The National Technology Transfer and Advancement Act, codified as a note to 15 U.S.C. 272, directs agencies to use voluntary consensus standards in their regulatory activities unless the agency provides Congress, through OMB, with an explanation of why using these standards would be inconsistent with applicable law or otherwise impractical. Voluntary consensus standards are technical standards (*e.g.*, specifications of materials, performance, design, or operation; test methods; sampling procedures; and related management systems practices) that are developed or adopted by voluntary consensus standards bodies. This proposed rule does not use technical standards. Therefore, CISA did not consider the use of voluntary consensus standards.

M. National Environmental Policy Act

Section 102 of the National Environmental Policy Act of 1969 (NEPA), 42 U.S.C. 4321 *et seq.*, requires Federal agencies to evaluate the impact of any proposed major Federal action significantly affecting the human environment, consider alternatives to the proposed action, provide public notice and opportunity for comment, and properly document its analysis. See 40 CFR parts 1501, 1502, 1506.6. DHS and its component agencies analyze proposed actions to determine whether NEPA applies and, if so, what level of analysis and documentation is required. See 40 CFR 1501.3.

DHS Directive 023–01 Rev. 01 (Directive) and Instruction Manual 023–01–001–01 Rev. 01 (Instruction Manual) together establish the policies and

procedures DHS and its component agencies use to comply with NEPA and the Council on Environmental Quality (CEQ) regulations for implementing the procedural requirements of NEPA, codified at 40 CFR parts 1500 through 1508.

The CEQ regulations allow Federal agencies to establish in their NEPA implementing procedures, with CEQ review and concurrence, categories of actions ("categorical exclusions") that experience has shown do not, individually or cumulatively, have a significant effect on the human environment and, therefore, do not require preparation of an Environmental Assessment or Environmental Impact Statement. 40 CFR 1507.3(e)(2)(ii), 1501.4. Appendix A of the Instruction Manual lists the DHS categorical exclusions. Under DHS NEPA implementing procedures, for a proposed action to be categorically excluded it must satisfy each of the following three conditions: (1) the entire action clearly fits within one or more of the categorical exclusions; (2) the action is not a piece of a larger action; and (3) no extraordinary circumstances exist that create the potential for a significant environmental effect. Instruction Manual section V.B(2)(a)–(c).

This proposed rule implements the authority in CIRCIA to develop and codify requirements for covered entities to report covered cyber incidents, ransom payments, and substantial new or different information from what was previously reported regarding such cyber incidents and ransom payments. The proposed rules will be codified at 6 CFR 226.1 through 226.20.

DHS has determined that this proposed rule will have no significant effect on the human environment and clearly fits within categorical exclusion A3 in Appendix A of the Instruction Manual established for promulgation of rules of a strictly administrative or procedural nature and that implement statutory requirements without substantive change.

This proposed rule is not part of a larger action and presents no extraordinary circumstances creating the potential for significant environmental effects. Therefore, this proposed rule is categorically excluded from further NEPA review.

VI. Proposed Regulation

List of Subjects in 6 CFR Part 226

Computer technology, Critical infrastructure, Cybersecurity, Internet, Reporting and recordkeeping requirements.

■ For the reasons stated in the preamble, and under the authority of 6 U.S.C. 681 through 681e and 6 U.S.C. 681g, the Department of Homeland Security proposes to add chapter II, consisting of part 226 to title 6 of the Code of Regulations to read as follows:

CHAPTER II—DEPARTMENT OF HOMELAND SECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

PART 226—COVERED CYBER INCIDENT AND RANSOM PAYMENT REPORTING

- Sec.
- 226.1 Definitions.
- 226.2 Applicability.
- 226.3 Required reporting on covered cyber incidents and ransom payments.
- 226.4 Exceptions to required reporting on covered cyber incidents and ransom payments.
- 226.5 CIRCIA Report submission deadlines.
- 226.6 Required manner and form of CIRCIA Reports.
- 226.7 Required information for CIRCIA Reports.
- 226.8 Required information for Covered Cyber Incident Reports.
- 226.9 Required information for Ransom Payment Reports.
- 226.10 Required information for Joint Covered Cyber Incident and Ransom Payment Reports.
- 226.11 Required information for Supplemental Reports.
- 226.12 Third party reporting procedures and requirements.
- 226.13 Data and records preservation requirements.
- 226.14 Request for information and subpoena procedures.
- 226.15 Civil enforcement of subpoenas.
- 226.16 Referral to the Department of Homeland Security Suspension and Debarment Official.
- 226.17 Referral to Cognizant Contracting Official or Attorney General.
- 226.18 Treatment of information and restrictions on use.
- 226.19 Procedures for protecting privacy and civil liberties.
- 226.20 Other procedural measures.

Authority: 6 U.S.C. 681–681e, 6 U.S.C. 681g; Sections 2240–2244 and 2246 of the Homeland Security Act of 2002, Pub. L. 107–296, 116 Stat. 2135, as amended by Pub. L. 117–103 and Pub. L. 117–263 (Dec. 23, 2022).

§ 226.1 Definitions.

For the purposes of this part:

CIRCIA means the Cyber Incident Reporting for Critical Infrastructure Act of 2022, as amended, in 6 U.S.C. 681–681g.

CIRCIA Agreement means an agreement between CISA and another Federal agency that meets the requirements of § 226.4(a)(2), has not expired or been terminated, and, when publicly posted by CISA in accordance

with § 226.4(a)(5), indicates the availability of a substantially similar reporting exception for use by a covered entity.

CIRCIA Report means a Covered Cyber Incident Report, Ransom Payment Report, Joint Covered Cyber Incident and Ransom Payment Report, or Supplemental Report, as defined under this part.

Cloud service provider means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in Nat'l Inst. of Standards & Tech., NIST Special Publication 800–145, and any amendatory or superseding document relating thereto.

Covered cyber incident means a substantial cyber incident experienced by a covered entity.

Covered Cyber Incident Report means a submission made by a covered entity or a third party on behalf of a covered entity to report a covered cyber incident as required by this part. A Covered Cyber Incident Report also includes any responses to optional questions and additional information voluntarily submitted as part of a Covered Cyber Incident Report.

Covered entity means an entity that meets the criteria set forth in § 226.2 of this part.

Cyber incident means an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or actually jeopardizes, without lawful authority, an information system.

Cybersecurity and Infrastructure Security Agency or CISA means the Cybersecurity and Infrastructure Security Agency as established under section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652), as amended by the Cybersecurity and Infrastructure Security Agency Act of 2018 and subsequent laws, or any successor organization.

Cybersecurity threat means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. This term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Director means the Director of CISA, any successors to that position within

the Department of Homeland Security, or any designee.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, including, but not limited to, operational technology systems such as industrial control systems, supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

Joint Covered Cyber Incident and Ransom Payment Report means a submission made by a covered entity or a third party on behalf of a covered entity to simultaneously report both a covered cyber incident and ransom payment related to the covered cyber incident being reported, as required by this part. A Joint Covered Cyber Incident and Ransom Payment Report also includes any responses to optional questions and additional information voluntarily submitted as part of the report.

Managed service provider means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity, such as hosting, or in a third-party data center.

Personal information means information that identifies a specific individual or nonpublic information associated with an identified or identifiable individual. Examples of personal information include, but are not limited to, photographs, names, home addresses, direct telephone numbers, social security numbers, medical information, personal financial information, contents of personal communications, and personal web browsing history.

Ransom payment means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

Ransom Payment Report means a submission made by a covered entity or a third party on behalf of a covered entity to report a ransom payment as required by this part. A Ransom Payment Report also includes any responses to optional questions and additional information voluntarily submitted as part of a Ransom Payment Report.

Ransomware attack means an occurrence that actually or imminently jeopardizes, without lawful authority,

the integrity, confidentiality, or availability of information on an information system, or that actually or imminently jeopardizes, without lawful authority, an information system that involves, but need not be limited to, the following:

- (1) The use or the threat of use of:
 - (i) Unauthorized or malicious code on an information system; or
 - (ii) Another digital mechanism such as a denial-of-service attack;
 - (2) To interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system; and
 - (3) To extort a ransom payment.
- (4) *Exclusion.* A ransomware attack does not include any event where the demand for a ransom payment is:
- (i) Not genuine; or
 - (ii) Made in good faith by an entity in response to a specific request by the owner or operator of the information system.

State, Local, Tribal, or Territorial Government entity or SLTT Government entity means an organized domestic entity which, in addition to having governmental character, has sufficient discretion in the management of its own affairs to distinguish it as separate from the administrative structure of any other governmental unit, and which is one of the following or a subdivision thereof:

- (1) A State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States;
- (2) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regardless of whether the council of governments is incorporated as a nonprofit corporation under State law, regional or interstate government entity, or agency or instrumentality of a Local government;
- (3) An Indian tribe, band, nation, or other organized group or community, or other organized group or community, including any Alaska Native village or regional or village corporation as defined in or established pursuant to 43 U.S.C. 1601 *et seq.*, which is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians; and
- (4) A rural community, unincorporated town or village, or other public entity.

Substantial cyber incident means a cyber incident that leads to any of the following:

- (1) A substantial loss of confidentiality, integrity or availability of a covered entity's information system or network;
- (2) A serious impact on the safety and resiliency of a covered entity's operational systems and processes;
- (3) A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;
- (4) Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a:
 - (i) Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or
 - (ii) Supply chain compromise.

(5) A "substantial cyber incident" resulting in the impacts listed in paragraphs (1) through (3) in this definition includes any cyber incident regardless of cause, including, but not limited to, any of the above incidents caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability.

(6) The term "substantial cyber incident" does not include:

- (i) Any lawfully authorized activity of a United States Government entity or SLTT Government entity, including activities undertaken pursuant to a warrant or other judicial process;
- (ii) Any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; or
- (iii) The threat of disruption as extortion, as described in 6 U.S.C. 650(22).

Supplemental report means a submission made by a covered entity or a third party on behalf of a covered entity to update or supplement a previously submitted Covered Cyber Incident Report or to report a ransom payment made by the covered entity after submitting a Covered Cyber Incident Report as required by this part. A supplemental report also includes any responses to optional questions and additional information voluntarily submitted as part of a supplemental report.

Supply chain compromise means a cyber incident within the supply chain of an information system that an

adversary can leverage, or does leverage, to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

Virtual currency means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value. Virtual currency includes a form of value that substitutes for currency or funds.

§ 226.2 Applicability.

This part applies to an entity in a critical infrastructure sector that either:

(a) *Exceeds the small business size standard.* Exceeds the small business size standard specified by the applicable North American Industry Classification System Code in the U.S. Small Business Administration's Small Business Size Regulations as set forth in 13 CFR part 121; or

(b) *Meets a sector-based criterion.* Meets one or more of the sector-based criteria provided below, regardless of the specific critical infrastructure sector of which the entity considers itself to be part:

(1) *Owns or operates a covered chemical facility.* The entity owns or operates a covered chemical facility subject to the Chemical Facility Anti-Terrorism Standards pursuant to 6 CFR part 27;

(2) *Provides wire or radio communications service.* The entity provides communications services by wire or radio communications, as defined in 47 U.S.C. 153(40), 153(59), to the public, businesses, or government, as well as one-way services and two-way services, including but not limited to:

- (i) Radio and television broadcasters;
- (ii) Cable television operators;
- (iii) Satellite operators;
- (iv) Telecommunications carriers;
- (v) Submarine cable licensees required to report outages to the Federal Communications Commission under 47 CFR 4.15;
- (vi) Fixed and mobile wireless service providers;
- (vii) Voice over internet Protocol providers; or
- (viii) internet service providers;

(3) *Owns or operates critical manufacturing sector infrastructure.* The entity owns or has business operations that engage in one or more of the following categories of manufacturing:

- (i) Primary metal manufacturing;
- (ii) Machinery manufacturing;
- (iii) Electrical equipment, appliance, and component manufacturing; or

(iv) Transportation equipment manufacturing;

(4) *Provides operationally critical support to the Department of Defense or processes, stores, or transmits covered defense information.* The entity is a contractor or subcontractor required to report cyber incidents to the Department of Defense pursuant to the definitions and requirements of the Defense Federal Acquisition Regulation Supplement 48 CFR 252.204–7012;

(5) *Performs an emergency service or function.* The entity provides one or more of the following emergency services or functions to a population equal to or greater than 50,000 individuals:

(i) Law enforcement;

(ii) Fire and rescue services;

(iii) Emergency medical services;

(iv) Emergency management; or

(v) Public works that contribute to public health and safety;

(6) *Bulk electric and distribution system entities.* The entity is required to report cybersecurity incidents under the North American Electric Reliability Corporation Critical Infrastructure Protection Reliability Standards or required to file an Electric Emergency Incident and Disturbance Report OE–417 form, or any successor form, to the Department of Energy;

(7) *Owens or operates financial services sector infrastructure.* The entity owns or operates any legal entity that qualifies as one or more of the following financial services entities:

(i) A banking or other organization regulated by:

(A) The Office of the Comptroller of the Currency under 12 CFR parts 30 and 53, which includes all national banks, Federal savings associations, and Federal branches and agencies of foreign banks;

(B) The Federal Reserve Board under: (1) 12 CFR parts 208, 211, 225, or 234, which includes all U.S. bank holding companies, savings and loans holding companies, state member banks, the U.S. operations of foreign banking organizations, Edge and agreement corporations, and certain designated financial market utilities; or

(2) 12 U.S.C. 248(j), which includes the Federal Reserve Banks;

(C) The Federal Deposit Insurance Corporation under 12 CFR part 304, which includes all insured state nonmember banks, insured state-licensed branches of foreign banks, and insured State savings associations;

(ii) A Federally insured credit union regulated by the National Credit Union Administration under 12 CFR part 748;

(iii) A designated contract market, swap execution facility, derivatives

clearing organization, or swap data repository regulated by the Commodity Futures Trading Commission under 17 CFR parts 37, 38, 39, and 49;

(iv) A futures commission merchant or swap dealer regulated by the Commodity Futures Trading Commission under 17 CFR parts 1 and 23;

(v) A systems compliance and integrity entity, security-based swap dealer, or security-based swap data repository regulated by the Securities and Exchange Commission under Regulation Systems Compliance and Integrity or Regulation Security-Based Swap Regulatory Regime, 17 CFR part 242;

(vi) A money services business as defined in 31 CFR 1010.100(ff); or

(vii) Fannie Mae and Freddie Mac as defined in 12 CFR 1201.1;

(8) *Qualifies as a State, local, Tribal, or territorial government entity.* The entity is a State, local, Tribal, or territorial government entity for a jurisdiction with a population equal to or greater than 50,000 individuals;

(9) *Qualifies as an education facility.* The entity qualifies as any of the following types of education facilities:

(i) A local educational agency, educational service agency, or state educational agency, as defined under 20 U.S.C. 7801, with a student population equal to or greater than 1,000 students; or

(ii) An institute of higher education that receives funding under Title IV of the Higher Education Act, 20 U.S.C. 1001 *et seq.*, as amended;

(10) *Involved with information and communications technology to support elections processes.* The entity manufactures, sells, or provides managed services for information and communications technology specifically used to support election processes or report and display results on behalf of State, Local, Tribal, or Territorial governments, including but not limited to:

(i) Voter registration databases;

(ii) Voting systems; and

(iii) Information and communication technologies used to report, display, validate, or finalize election results;

(11) *Provides essential public health-related services.* The entity provides one or more of the following essential public health-related services:

(i) Owns or operates a hospital, as defined by 42 U.S.C. 1395x(e), with 100 or more beds, or a critical access hospital, as defined by 42 U.S.C. 1395x(mm)(1);

(ii) Manufactures drugs listed in appendix A of the *Essential Medicines Supply Chain and Manufacturing*

Resilience Assessment developed pursuant to section 3 of E.O. 14017; or

(iii) Manufactures a Class II or Class III device as defined by 21 U.S.C. 360c;

(12) *Information technology entities.* The entity meets one or more of the following criteria:

(i) Knowingly provides or supports information technology hardware, software, systems, or services to the Federal government;

(ii) Has developed and continues to sell, license, or maintain any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

(A) Is designed to run with elevated privilege or manage privileges;

(B) Has direct or privileged access to networking or computing resources;

(C) Is designed to control access to data or operational technology;

(D) Performs a function critical to trust; or

(E) Operates outside of normal trust boundaries with privileged access;

(iii) Is an original equipment manufacturer, vendor, or integrator of operational technology hardware or software components;

(iv) Performs functions related to domain name operations;

(13) *Owens or operates a commercial nuclear power reactor or fuel cycle Facility.* The entity owns or operates a commercial nuclear power reactor or fuel cycle facility licensed to operate under the regulations of the Nuclear Regulatory Commission, 10 CFR chapter I;

(14) *Transportation system entities.* The entity is required by the Transportation Security Administration to report cyber incidents or otherwise qualifies as one or more of the following transportation system entities:

(i) A freight railroad carrier identified in 49 CFR 1580.1(a)(1), (4), or (5);

(ii) A public transportation agency or passenger railroad carrier identified in 49 CFR 1582.1(a)(1)–(4);

(iii) An over-the-road bus operator identified in 49 CFR 1584.1;

(iv) A pipeline facility or system owner or operator identified in 49 CFR 1586.101;

(v) An aircraft operator regulated under 49 CFR part 1544;

(vi) An indirect air carrier regulated under 49 CFR part 1548;

(vii) An airport operator regulated under 49 CFR part 1542; or

(viii) A Certified Cargo Screening Facility regulated under 49 CFR part 1549;

(15) *Subject to regulation under the Maritime Transportation Security Act.* The entity owns or operates a vessel,

facility, or outer continental shelf facility subject to 33 CFR parts 104, 105, or 106; or

(16) *Owens or operates a qualifying community water system or publicly owned treatment works.* The entity owns or operates a community water system, as defined in 42 U.S.C. 300f(15), or a publicly owned treatment works, as defined in 40 CFR 403.3(q), for a population greater than 3,300 people.

§ 226.3 Required reporting on covered cyber incidents and ransom payments.

(a) *Covered cyber incident.* A covered entity that experiences a covered cyber incident must report the covered cyber incident to CISA in accordance with this part.

(b) *Ransom payment.* A covered entity that makes a ransom payment, or has another entity make a ransom payment on the covered entity's behalf, as the result of a ransomware attack against the covered entity must report the ransom payment to CISA in accordance with this part. This reporting requirement applies to a covered entity even if the ransomware attack that resulted in a ransom payment is not a covered cyber incident subject to the reporting requirements of this part. If a covered entity makes a ransom payment that relates to a covered cyber incident that was previously reported in accordance with paragraph (a) of this section, the covered entity must instead submit a supplemental report in accordance with paragraph (d)(1)(ii) of this section.

(c) *Covered cyber incident and ransom payment.* A covered entity that experiences a covered cyber incident and makes a ransom payment, or has another entity make a ransom payment on the covered entity's behalf, that is related to that covered cyber incident may report both events to CISA in a Joint Covered Cyber Incident and Ransom Payment Report in accordance with this part. If a covered entity, or a third party acting on the covered entity's behalf, submits a Joint Covered Cyber Incident and Ransom Payment Report in accordance with this part, the covered entity is not required to also submit reports pursuant to paragraph (a) and (b) of this section.

(d) *Supplemental Reports—(1) Required Supplemental Reports.* A covered entity must promptly submit Supplemental Reports to CISA about a previously reported covered cyber incident in accordance with this part unless and until such date that the covered entity notifies CISA that the covered cyber incident at issue has concluded and has been fully mitigated and resolved. Supplemental Reports

must be promptly submitted by the covered entity if:

(i) Substantial new or different information becomes available. Substantial new or different information includes but is not limited to any information that the covered entity was required to provide as part of a Covered Cyber Incident Report but did not have at the time of submission; or

(ii) The covered entity makes a ransom payment, or has another entity make a ransom payment on the covered entity's behalf, that relates to a covered cyber incident that was previously reported in accordance with paragraph (a) of this section.

(2) *Optional notification that a covered cyber incident has concluded.*

A covered entity may submit a Supplemental Report to inform CISA that a covered cyber incident previously reported in accordance with paragraph (a) of this section has concluded and been fully mitigated and resolved.

§ 226.4 Exceptions to required reporting on covered cyber incidents and ransom payments.

(a) *Substantially similar reporting exception—(1) In general.* A covered entity that reports a covered cyber incident, ransom payment, or information that must be submitted to CISA in a supplemental report to another Federal agency pursuant to the terms of a CIRCIA Agreement will satisfy the covered entity's reporting obligations under § 226.3. A covered entity is responsible for confirming that a CIRCIA Agreement is applicable to the covered entity and the specific reporting obligation it seeks to satisfy under this part, and therefore, qualifies for this exemption.

(2) *CIRCIA Agreement requirements.* A CIRCIA Agreement may be entered into and maintained by CISA and another Federal agency in circumstances where CISA has determined the following:

(i) A law, regulation, or contract exists that requires one or more covered entities to report covered cyber incidents or ransom payments to the other Federal agency;

(ii) The required information that a covered entity must submit to the other Federal agency pursuant to a legal, regulatory, or contractual reporting requirement is substantially similar information to that which a covered entity is required to include in a CIRCIA Report as specified in §§ 226.7 through 226.11, as applicable;

(iii) The applicable law, regulation, or contract requires covered entities to report covered cyber incidents or ransom payments to the other Federal

agency within a substantially similar timeframe to those for CIRCIA Reports specified in § 226.5; and

(iv) CISA and the other Federal agency have an information sharing mechanism in place.

(3) *Substantially similar information determination.* CISA retains discretion to determine what constitutes substantially similar information for the purposes of this part. In general, in making this determination, CISA will consider whether the specific fields of information reported by the covered entity to another Federal agency are functionally equivalent to the fields of information required to be reported in CIRCIA Reports under §§ 226.7 through 226.11, as applicable.

(4) *Substantially similar timeframe.* Reporting in a substantially similar timeframe means that a covered entity is required to report covered cyber incidents, ransom payments, or supplemental reports to another Federal agency in a timeframe that enables the report to be shared by the Federal agency with CISA by the applicable reporting deadline specified for each type of CIRCIA Report under § 226.5.

(5) *Public posting of CIRCIA Agreements.* CISA will maintain an accurate catalog of all CIRCIA Agreements on a public-facing website and will make CIRCIA Agreements publicly available, to the maximum extent practicable. An agreement will be considered a CIRCIA Agreement for the purposes of this section when CISA publishes public notice concerning the agreement on such website and until notice of termination or expiration has been posted as required under § 226.4(a)(6).

(6) *Termination or expiration of a CIRCIA Agreement.* CISA may terminate a CIRCIA Agreement at any time. CISA will provide notice of the termination or expiration of CIRCIA Agreements on the public-facing website where the catalog of CIRCIA Agreements is maintained.

(7) *Continuing supplemental reporting requirement.* Covered entities remain subject to the supplemental reporting requirements specified under § 226.3(d), unless the covered entity submits the required information to another Federal agency pursuant to the terms of a CIRCIA Agreement.

(8) *Communications with CISA.* Nothing in this section prevents or otherwise restricts CISA from contacting any entity that submits information to another Federal agency, nor is any entity prevented from communicating with, or submitting a CIRCIA Report to, CISA.

(b) *Domain Name System exception.* The following entities, to the degree that

they are considered a covered entity under § 226.2, are exempt from the reporting requirements in this part:

(1) The Internet Corporation for Assigned Names and Numbers;

(2) The American Registry for Internet Numbers;

(3) Any affiliates controlled by the covered entities listed in paragraphs (b)(1) and (2) of this section; and

(4) The root server operator function of a covered entity that has been recognized by the Internet Corporation for Assigned Names and Numbers as responsible for operating one of the root identities and has agreed to follow the service expectations established by the Internet Corporation for Assigned Names and Numbers and its Root Server System Advisory Committee.

(c) *FISMA report exception.* Federal agencies that are required by the Federal Information Security Modernization Act, 44 U.S.C. 3551 *et seq.*, to report incidents to CISA are exempt from reporting those incidents as covered cyber incidents under this part.

§ 226.5 CIRCIA Report submission deadlines.

Covered entities must submit CIRCIA Reports in accordance with the submission deadlines specified in this section.

(a) *Covered Cyber Incident Report deadline.* A covered entity must submit a Covered Cyber Incident Report to CISA no later than 72 hours after the covered entity reasonably believes the covered cyber incident has occurred.

(b) *Ransom Payment Report deadline.* A covered entity must submit a Ransom Payment Report to CISA no later than 24 hours after the ransom payment has been disbursed.

(c) *Joint Covered Cyber Incident and Ransom Payment Report deadline.* A covered entity that experiences a covered cyber incident and makes a ransom payment within 72 hours after the covered entity reasonably believes a covered cyber incident has occurred may submit a Joint Covered Cyber Incident and Ransom Payment Report to CISA no later than 72 hours after the covered entity reasonably believes the covered cyber incident has occurred.

(d) *Supplemental Report Deadline.* A covered entity must promptly submit supplemental reports to CISA. If a covered entity submits a supplemental report on a ransom payment made after the covered entity submitted a Covered Cyber Incident Report, as required by § 226.3(d)(1)(ii), the covered entity must submit the Supplemental Report to CISA no later than 24 hours after the ransom payment has been disbursed.

§ 226.6 Required manner and form of CIRCIA Reports.

A covered entity must submit CIRCIA Reports to CISA through the web-based CIRCIA Incident Reporting Form available on CISA's website or in any other manner and form of reporting approved by the Director.

§ 226.7 Required information for CIRCIA Reports.

A covered entity must provide the following information in all CIRCIA Reports to the extent such information is available and applicable to the event reported:

(a) Identification of the type of CIRCIA Report submitted by the covered entity;

(b) Information relevant to establishing the covered entity's identity, including the covered entity's:

(1) Full legal name;

(2) State of incorporation or formation;

(3) Affiliated trade names;

(4) Organizational entity type;

(5) Physical address;

(6) website;

(7) Internal incident tracking number for the reported event;

(8) Applicable business numerical identifiers;

(9) Name of the parent company or organization, if applicable; and

(10) The critical infrastructure sector or sectors in which the covered entity considers itself to be included;

(c) Contact information, including the full name, email address, telephone number, and title for:

(1) The individual submitting the CIRCIA Report on behalf of the covered entity;

(2) A point of contact for the covered entity if the covered entity uses a third party to submit the CIRCIA Report or would like to designate a preferred point of contact that is different from the individual submitting the report; and

(3) A registered agent for the covered entity, if neither the individual submitting the CIRCIA Report, nor the designated preferred point of contact are a registered agent for the covered entity; and

(d) If a covered entity uses a third party to submit a CIRCIA Report on the covered entity's behalf, an attestation that the third party is expressly authorized by the covered entity to submit the CIRCIA Report on the covered entity's behalf.

§ 226.8 Required information for Covered Cyber Incident Reports.

A covered entity must provide all the information identified in § 226.7 and the

following information in a Covered Cyber Incident Report, to the extent such information is available and applicable to the covered cyber incident:

(a) A description of the covered cyber incident, including but not limited to:

(1) Identification and description of the function of the affected networks, devices, and/or information systems that were, or are reasonably believed to have been, affected by the covered cyber incident, including but not limited to:

(i) Technical details and physical locations of such networks, devices, and/or information systems; and

(ii) Whether any such information system, network, and/or device supports any elements of the intelligence community or contains information that has been determined by the United States Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in 42 U.S.C. 2014(y);

(2) A description of any unauthorized access, regardless of whether the covered cyber incident involved an attributed or unattributed cyber intrusion, identification of any informational impacts or information compromise, and any network location where activity was observed;

(3) Dates pertaining to the covered cyber incident, including but not limited to:

(i) The date the covered cyber incident was detected;

(ii) The date the covered cyber incident began;

(iii) If fully mitigated and resolved at the time of reporting, the date the covered cyber incident ended;

(iv) The timeline of compromised system communications with other systems; and

(v) For covered cyber incidents involving unauthorized access, the suspected duration of the unauthorized access prior to detection and reporting; and

(4) The impact of the covered cyber incident on the covered entity's operations, such as information related to the level of operational impact and direct economic impacts to operations; any specific or suspected physical or informational impacts; and information to enable CISA's assessment of any known impacts to national security or public health and safety;

(b) The category or categories of any information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person or persons;

(c) A description of any vulnerabilities exploited, including but not limited to the specific products or technologies and versions of the products or technologies in which the vulnerabilities were found;

(d) A description of the covered entity's security defenses in place, including but not limited to any controls or measures that resulted in the detection or mitigation of the incident;

(e) A description of the type of incident and the tactics, techniques, and procedures used to perpetrate the covered cyber incident, including but not limited to any tactics, techniques, and procedures used to gain initial access to the covered entity's information systems, escalate privileges, or move laterally, if applicable;

(f) Any indicators of compromise, including but not limited to those listed in § 226.13(b)(1)(ii), observed in connection with the covered cyber incident;

(g) A description and, if possessed by the covered entity, a copy or samples of any malicious software the covered entity believes is connected with the covered cyber incident;

(h) Any identifying information, including but not limited to all available contact information, for each actor reasonably believed by the covered entity to be responsible for the covered cyber incident;

(i) A description of any mitigation and response activities taken by the covered entity in response to the covered cyber incident, including but not limited to:

(1) Identification of the current phase of the covered entity's incident response efforts at the time of reporting;

(2) The covered entity's assessment of the effectiveness of response efforts in mitigating and responding to the covered cyber incident;

(3) Identification of any law enforcement agency that is engaged in responding to the covered cyber incident, including but not limited to information about any specific law enforcement official or point of contact, notifications received from law enforcement, and any law enforcement agency that the covered entity otherwise believes may be involved in investigating the covered cyber incident; and

(4) Whether the covered entity requested assistance from another entity in responding to the covered cyber incident and, if so, the identity of each entity and a description of the type of assistance requested or received from each entity;

(j) Any other data or information as required by the web-based CIRCIA Incident Reporting Form or any other

manner and form of reporting authorized under § 226.6.

§ 226.9 Required information for Ransom Payment Reports.

A covered entity must provide all the information identified in § 226.7 and the following information in a Ransom Payment Report, to the extent such information is available and applicable to the ransom payment:

(a) A description of the ransomware attack, including but not limited to:

(1) Identification and description of the function of the affected networks, devices, and/or information systems that were, or are reasonably believed to have been, affected by the ransomware attack, including but not limited to:

(i) Technical details and physical locations of such networks, devices, and/or information systems; and

(ii) Whether any such information system, network, and/or device supports any elements of the intelligence community or contains information that has been determined by the United States Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in 42 U.S.C. 2014(y);

(2) A description of any unauthorized access, regardless of whether the ransomware attack involved an attributed or unattributed cyber intrusion, identification of any informational impacts or information compromise, and any network location where activity was observed;

(3) Dates pertaining to the ransomware attack, including but not limited to:

(i) The date the ransomware attack was detected;

(ii) The date the ransomware attack began;

(iii) If fully mitigated and resolved at the time of reporting, the date the ransomware attack ended;

(iv) The timeline of compromised system communications with other systems; and

(v) For ransomware attacks involving unauthorized access, the suspected duration of the unauthorized access prior to detection and reporting; and

(4) The impact of the ransomware attack on the covered entity's operations, such as information related to the level of operational impact and direct economic impacts to operations; any specific or suspected physical or informational impacts; and any known or suspected impacts to national security or public health and safety;

(b) A description of any vulnerabilities exploited, including but

not limited to the specific products or technologies and versions of the products or technologies in which the vulnerabilities were found;

(c) A description of the covered entity's security defenses in place, including but not limited to any controls or measures that resulted in the detection or mitigation of the ransomware attack;

(d) A description of the tactics, techniques, and procedures used to perpetrate the ransomware attack, including but not limited to any tactics, techniques, and procedures used to gain initial access to the covered entity's information systems, escalate privileges, or move laterally, if applicable;

(e) Any indicators of compromise the covered entity believes are connected with the ransomware attack, including, but not limited to, those listed in section 226.13(b)(1)(ii), observed in connection with the ransomware attack;

(f) A description and, if possessed by the covered entity, a copy or sample of any malicious software the covered entity believes is connected with the ransomware attack;

(g) Any identifying information, including but not limited to all available contact information, for each actor reasonably believed by the covered entity to be responsible for the ransomware attack;

(h) The date of the ransom payment;

(i) The amount and type of assets used in the ransom payment;

(j) The ransom payment demand, including but not limited to the type and amount of virtual currency, currency, security, commodity, or other form of payment requested;

(k) The ransom payment instructions, including but not limited to information regarding how to transmit the ransom payment; the virtual currency or physical address where the ransom payment was requested to be sent; any identifying information about the ransom payment recipient; and information related to the completed payment, including any transaction identifier or hash;

(l) Outcomes associated with making the ransom payment, including but not limited to whether any exfiltrated data was returned or a decryption capability was provided to the covered entity, and if so, whether the decryption capability was successfully used by the covered entity;

(m) A description of any mitigation and response activities taken by the covered entity in response to the ransomware attack, including but not limited to:

(1) Identification of the current phase of the covered entity's incident response efforts at the time of reporting;

(2) The covered entity's assessment of the effectiveness of response efforts in mitigating and responding to the ransomware attack;

(3) Identification of any law enforcement agency that is engaged in responding to the ransomware attack, including but not limited to information about any specific law enforcement official or point of contact, notifications received from law enforcement, and any law enforcement agency that the covered entity otherwise believes may be involved in investigating the ransomware attack; and

(4) Whether the covered entity requested assistance from another entity in responding to the ransomware attack or making the ransom payment and, if so, the identity of such entity or entities and a description of the type of assistance received from each entity;

(n) Any other data or information as required by the web-based CIRCIA Incident Reporting Form or any other manner and form of reporting authorized under § 226.6.

§ 226.10 Required information for Joint Covered Cyber Incident and Ransom Payment Reports.

A covered entity must provide all the information identified in §§ 226.7, 226.8, and 226.9 in a Joint Covered Cyber Incident and Ransom Payment Report to the extent such information is available and applicable to the reported covered cyber incident and ransom payment.

§ 226.11 Required information for Supplemental Reports.

(a) *In general.* A covered entity must include all of the information identified as required in § 226.7 and the following information in any Supplemental Report:

(1) The case identification number provided by CISA for the associated Covered Cyber Incident Report or Joint Covered Cyber Incident and Ransom Payment Report;

(2) The reason for filing the Supplemental Report;

(3) Any substantial new or different information available about the covered cyber incident, including but not limited to information the covered entity was required to provide as part of a Covered Cyber Incident Report but did not have at the time of submission and information required under § 226.9 if the covered entity or another entity on the covered entity's behalf has made a ransom payment after submitting a Covered Cyber Incident Report; and

(4) Any other data or information required by the web-based CIRCIA Incident Reporting Form or any other manner and form of reporting authorized under § 226.6.

(b) *Required information for a Supplemental Report providing notice of a ransom payment made following submission of a Covered Cyber Incident Report.* When a covered entity submits a Supplemental Report to notify CISA that the covered entity has made a ransom payment after submitting a related Covered Cyber Incident Report, the supplemental report must include the information required in § 226.9.

(c) *Optional information to provide notification that a covered cyber incident has concluded.* Covered entities that choose to submit a notification to CISA that a covered cyber incident has concluded and has been fully mitigated and resolved may submit optional information related to the conclusion of the covered cyber incident.

§ 226.12 Third party reporting procedures and requirements.

(a) *General.* A covered entity may expressly authorize a third party to submit a CIRCIA Report on the covered entity's behalf to satisfy the covered entity's reporting obligations under § 226.3. The covered entity remains responsible for ensuring compliance with its reporting obligations under this part even when the covered entity has authorized a third party to submit a CIRCIA Report on the covered entity's behalf.

(b) *Procedures for third party submission of CIRCIA Reports.* CIRCIA Reports submitted by third parties must comply with the reporting requirements and procedures for covered entities set forth in this part.

(c) *Confirmation of express authorization required.* For the purposes of compliance with the covered entity's reporting obligations under this part, upon submission of a CIRCIA Report, a third party must confirm that the covered entity expressly authorized the third party to file the CIRCIA Report on the covered entity's behalf. CIRCIA Reports submitted by a third party without an attestation from the third party that the third party has the express authorization of a covered entity to submit a report on the covered entity's behalf will not be considered by CISA for the purposes of compliance of the covered entity's reporting obligations under this part.

(d) *Third party ransom payments and responsibility to advise a covered entity.* A third party that makes a ransom payment on behalf of a covered entity

impacted by a ransomware attack is not required to submit a Ransom Payment Report on behalf of itself for the ransom payment. When a third party knowingly makes a ransom payment on behalf of a covered entity, the third party must advise the covered entity of its obligations to submit a Ransom Payment Report under this part.

§ 226.13 Data and records preservation requirements.

(a) *Applicability.* (1) A covered entity that is required to submit a CIRCIA Report under § 226.3 or experiences a covered cyber incident or makes a ransom payment but is exempt from submitting a CIRCIA Report pursuant to § 226.4(a) is required to preserve data and records related to the covered cyber incident or ransom payment in accordance with this section.

(2) A covered entity maintains responsibility for compliance with the preservation requirements in this section regardless of whether the covered entity submitted a CIRCIA Report or a third party submitted the CIRCIA Report on the covered entity's behalf.

(b) *Covered data and records.* (1) A covered entity must preserve the following data and records:

(i) Communications with any threat actor, including copies of actual correspondence, including but not limited to emails, texts, instant or direct messages, voice recordings, or letters; notes taken during any interactions; and relevant information on the communication facilities used, such as email or Tor site;

(ii) Indicators of compromise, including but not limited to suspicious network traffic; suspicious files or registry entries; suspicious emails; unusual system logins; unauthorized accounts created, including usernames, passwords, and date/time stamps and time zones for activity associated with such accounts; and copies or samples of any malicious software;

(iii) Relevant log entries, including but not limited to, Domain Name System, firewall, egress, packet capture file, NetFlow, Security Information and Event Management/Security Information Management, database, Intrusion Prevention System/Intrusion Detection System, endpoint, Active Directory, server, web, Virtual Private Network, Remote Desktop Protocol, and Window Event;

(iv) Relevant forensic artifacts, including but not limited to live memory captures; forensic images; and preservation of hosts pertinent to the incident;

(v) Network data, including but not limited to NetFlow or packet capture file, and network information or traffic related to the incident, including the internet Protocol addresses associated with the malicious cyber activity and any known corresponding dates, timestamps, and time zones;

(vi) Data and information that may help identify how a threat actor compromised or potentially compromised an information system, including but not limited to information indicating or identifying how one or more threat actors initially obtained access to a network or information system and the methods such actors employed during the incident;

(vii) System information that may help identify exploited vulnerabilities, including but not limited to operating systems, version numbers, patch levels, and configuration settings;

(viii) Information about exfiltrated data, including but not limited to file names and extensions; the amount of data exfiltration by byte value; category of data exfiltrated, including but not limited to, classified, proprietary, financial, or personal information; and evidence of exfiltration, including but not limited to relevant logs and screenshots of exfiltrated data sent from the threat actor;

(ix) All data or records related to the disbursement or payment of any ransom payment, including but not limited to pertinent records from financial accounts associated with the ransom payment; and

(x) Any forensic or other reports concerning the incident, whether internal or prepared for the covered entity by a cybersecurity company or other third-party vendor.

(2) A covered entity is not required to create any data or records it does not already have in its possession based on this requirement.

(c) *Required preservation period.* Covered entities must preserve all data and records identified in paragraph (b) of this section:

(1) Beginning on the earliest of the following dates:

(i) The date upon which the covered entity establishes a reasonable belief that a covered cyber incident occurred; or

(ii) The date upon which a ransom payment was disbursed; and

(2) For no less than two years from the submission of the most recently required CIRCIA Report submitted pursuant to § 226.3, or from the date such submission would have been required but for the exception pursuant to § 226.4(a).

(d) *Original data or record format.* Covered entities must preserve data and records set forth in paragraph (b) of this section in their original format or form whether the data or records are generated automatically or manually, internally or received from outside sources by the covered entity, and regardless of the following:

(1) Form or format, including hard copy records and electronic records;

(2) Where the information is stored, located, or maintained without regard to the physical location of the information, including stored in databases or cloud storage, on network servers, computers, other wireless devices, or by a third-party on behalf of the covered entity; and

(3) Whether the information is in active use or archived.

(e) *Storage, protection, and allowable use of data and records.* (1) A covered entity may select its own storage methods, electronic or non-electronic, and procedures to maintain the data and records that must be preserved under this section.

(2) Data and records must be readily accessible, retrievable, and capable of being lawfully shared by the covered entity, including in response to a lawful government request.

(3) A covered entity must use reasonable safeguards to protect data and records against unauthorized access or disclosure, deterioration, deletion, destruction, and alteration.

§ 226.14 Request for information and subpoena procedures.

(a) *In general.* This section applies to covered entities, except a covered entity that qualifies as a State, Local, Tribal, or Territorial Government entity as defined in § 226.1.

(b) *Use of authorities.* When determining whether to exercise the authorities in this section, the Director or designee will take into consideration:

(1) The complexity in determining if a covered cyber incident has occurred; and

(2) The covered entity's prior interaction with CISA or the covered entity's awareness of CISA's policies and procedures for reporting covered cyber incidents and ransom payments.

(c) *Request for information—(1) Issuance of request.* The Director may issue a request for information to a covered entity if there is reason to believe that the entity experienced a covered cyber incident or made a ransom payment but failed to report the incident or payment in accordance with § 226.3. Reason to believe that a covered entity failed to submit a CIRCIA Report in accordance with § 226.3 may be

based upon public reporting or other information in possession of the Federal Government, which includes but is not limited to analysis performed by CISA. A request for information will be served on a covered entity in accordance with the procedures in paragraph (e) of this section.

(2) *Form and contents of the request.* At a minimum, a request for information must include:

(i) The name and address of the covered entity;

(ii) A summary of the facts that have led CISA to believe that the covered entity has failed to submit a required CIRCIA Report in accordance with § 226.3. This summary is subject to the nondisclosure provision in paragraph (f) of this section;

(iii) A description of the information requested from the covered entity. The Director, in his or her discretion, may decide the scope and nature of information necessary for CISA to confirm whether a covered cyber incident or ransom payment occurred. Requested information may include electronically stored information, documents, reports, verbal or written responses, records, accounts, images, data, data compilations, and tangible items;

(iv) A date by which the covered entity must reply to the request for information; and

(v) The manner and format in which the covered entity must provide all information requested to CISA.

(3) *Response to request for information.* A covered entity must reply in the manner and format, and by the deadline, specified by the Director. If the covered entity does not respond by the date specified in paragraph (c)(2)(iv) of this section or the Director determines that the covered entity's response is inadequate, the Director, in his or her discretion, may request additional information from the covered entity to confirm whether a covered cyber incident or ransom payment occurred, or the Director may issue a subpoena to compel information from the covered entity pursuant to paragraph (d) of this section.

(4) *Treatment of information received.* Information provided to CISA by a covered entity in a reply to a request for information under this section will be treated in accordance with §§ 226.18 and 226.19.

(5) *Unavailability of Appeal.* A request for information is not a final agency action within the meaning of 5 U.S.C. 704 and cannot be appealed.

(d) *Subpoena—(1) Issuance of subpoena.* The Director may issue a subpoena to compel disclosure of

information from a covered entity if the entity fails to reply by the date specified in paragraph (c)(2)(iv) of this section or provides an inadequate response, to a request for information. The authority to issue a subpoena is a nondelegable authority. A subpoena will be served on a covered entity in accordance with the procedures in paragraph (e) of this section.

(2) *Timing of subpoena.* A subpoena to compel disclosure of information from a covered entity may be issued no earlier than 72 hours after the date of service of the request for information.

(3) *Form and contents of subpoena.* At a minimum, a subpoena must include:

(i) The name and address of the covered entity;

(ii) An explanation of the basis for issuance of the subpoena and a copy of the request for information previously issued to the covered entity, subject to the nondisclosure provision in paragraph (f) of this section;

(iii) A description of the information that the covered entity is required to produce. The Director, in his or her discretion, may determine the scope and nature of information necessary to determine whether a covered cyber incident or ransom payment occurred, obtain the information required to be reported under § 226.3, and to assess the potential impacts to national security, economic security, or public health and safety. Subpoenaed information may include electronically stored information, documents, reports, verbal or written responses, records, accounts, images, data, data compilations, and tangible items;

(iv) A date by which the covered entity must reply; and

(v) The manner and format in which the covered entity must provide all information requested to CISA.

(4) *Reply to the Subpoena.* A covered entity must reply in the manner and format, and by the deadline, specified by the Director. If the Director determines that the information received from the covered entity is inadequate to determine whether a covered cyber incident or ransom payment occurred, does not satisfy the reporting requirements under § 226.3, or is inadequate to assess the potential impacts to national security, economic security, or public health and safety, the Director may request or subpoena additional information from the covered entity or request civil enforcement of a subpoena pursuant to § 226.15.

(5) *Authentication requirement for electronic subpoenas.* Subpoenas issued electronically must be authenticated with a cryptographic digital signature of

an authorized representative of CISA or with a comparable successor technology that demonstrates the subpoena was issued by CISA and has not been altered or modified since issuance. Electronic subpoenas that are not authenticated pursuant to this subparagraph are invalid.

(6) *Treatment of information received in response to a subpoena—(i) In general.* Information obtained by subpoena is not subject to the information treatment requirements and restrictions imposed within § 226.18 and privacy and procedures for protecting privacy and civil liberties in § 226.19; and

(ii) *Provision of certain information for criminal prosecution and regulatory enforcement proceedings.* The Director may provide information submitted in response to a subpoena to the Attorney General or the head of a Federal regulatory agency if the Director determines that the facts relating to the cyber incident or ransom payment may constitute grounds for criminal prosecution or regulatory enforcement action. The Director may consult with the Attorney General or the head of the appropriate Federal regulatory agency when making any such determination. Information provided by CISA under this paragraph (d)(6)(ii) may be used by the Attorney General or the head of a Federal regulatory agency for criminal prosecution or a regulatory enforcement action. Any decision by the Director to exercise this authority does not constitute final agency action within the meaning of 5 U.S.C. 704 and cannot be appealed.

(7) *Withdrawal and appeals of subpoena issuance—(i) In general.* CISA, in its discretion, may withdraw a subpoena that is issued to a covered entity. Notice of withdrawal of a subpoena will be served on a covered entity in accordance with the procedures in paragraph (e) of this section.

(ii) *Appeals of subpoena issuance.* A covered entity may appeal the issuance of a subpoena through a written request that the Director withdraw it. A covered entity, or a representative on behalf of the covered entity, must file a Notice of Appeal within seven (7) calendar days after service of the subpoena. All Notices of Appeal must include:

(A) The name of the covered entity;

(B) The date of subpoena issuance;

(C) A clear request that the Director withdraw the subpoena;

(D) The covered entity's rationale for requesting a withdrawal of the subpoena; and

(E) Any additional information that the covered entity would like the

Director to consider as part of the covered entity's appeal.

(iii) *Director's final decision.* Following receipt of a Notice of Appeal, the Director will issue a final decision and serve it upon the covered entity. A final decision made by the Director constitutes final agency action. If the Director's final decision is to withdraw the subpoena, a notice of withdrawal of a subpoena will be served on the covered entity in accordance with the procedures in § 226.14(e).

(e) *Service—(1) covered entity point of contact.* A request for information, subpoena, or notice of withdrawal of a subpoena may be served by delivery on an officer, managing or general agent, or any other agent authorized by appointment or law to receive service of process on behalf of the covered entity.

(2) *Method of service.* Service of a request for information, subpoena, or notice of withdrawal of a subpoena will be served on a covered entity through a reasonable electronic or non-electronic attempt that demonstrates receipt, such as certified mail with return receipt, express commercial courier delivery, or electronically.

(3) *Date of service.* The date of service of any request for information, subpoena, or notice of withdrawal of a subpoena shall be the date on which the document is mailed, electronically transmitted, or delivered in person, whichever is applicable.

(f) *Nondisclosure of certain information.* In connection with the procedures in this section, CISA will not disclose classified information as defined in Section 1.1(d) of E.O. 12968 and reserves the right to not disclose any other information or material that is protected from disclosure under law or policy.

§ 226.15 Civil enforcement of subpoenas.

(a) *In general.* If a covered entity fails to comply with a subpoena issued pursuant to § 226.14(d), the Director may refer the matter to the Attorney General to bring a civil action to enforce the subpoena in any United States District Court for the judicial district in which the covered entity resides, is found, or does business.

(b) *Contempt.* A United States District Court may order compliance with the subpoena and punish failure to obey a subpoena as a contempt of court.

(c) *Classified and protected information.* In any review of an action taken under § 226.14, if the action was based on classified or protected information as described in § 226.14(f), such information may be submitted to the reviewing court *ex parte* and *in camera*. This paragraph does not confer

or imply any right to review in any tribunal, judicial or otherwise.

§ 226.16 Referral to the Department of Homeland Security Suspension and Debarment Official.

The Director must refer all circumstances concerning a covered entity's noncompliance that may warrant suspension and debarment action to the Department of Homeland Security Suspension and Debarment Official.

§ 226.17 Referral to Cognizant Contracting Official or Attorney General.

The Director may refer information concerning a covered entity's noncompliance with the reporting requirements in this part that pertain to performance under a federal procurement contract to the cognizant contracting official or the Attorney General for civil or criminal enforcement.

§ 226.18 Treatment of information and restrictions on use.

(a) *In general.* The protections and restrictions on use enumerated in this section apply to CIRCIA Reports and information included in such reports where specified in this section, as well as to all responses provided to requests for information issued under § 226.14(c). This section does not apply to information and reports submitted in response to a subpoena issued under § 226.14(d) or following Federal government action under §§ 226.15–226.17.

(b) *Treatment of information—(1) Designation as commercial, financial, and proprietary information.* A covered entity must clearly designate with appropriate markings at the time of submission a CIRCIA Report, a response provided to a request for information issued under § 226.14(c), or any portion of a CIRCIA Report or a response provided to a request for information issued under § 226.14(c) that it considers to be commercial, financial, and proprietary information. CIRCIA Reports, responses provided to a request for information issued under § 226.14(c), or designated portions thereof, will be treated as commercial, financial, and proprietary information of the covered entity upon designation as such by a covered entity.

(2) *Exemption from disclosure under the Freedom of Information Act.* CIRCIA Reports submitted pursuant to this part and responses provided to requests for information issued under § 226.14(c) are exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(3), and under any State, Local, or Tribal government freedom of

information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records. If CISA receives a request under the Freedom of Information Act to which a CIRCIA Report, response to a request for information under § 226.14(c), or information contained therein is responsive, CISA will apply all applicable exemptions from disclosure, consistent with 6 CFR part 5.

(3) *No Waiver of Privilege.* A covered entity does not waive any applicable privilege or protection provided by law, including trade secret protection, as a consequence of submitting a CIRCIA Report under this part or a response to a request for information issued under § 226.14(c).

(4) *Ex parte communications waiver.* CIRCIA Reports submitted pursuant to this part and responses provided to requests for information issued under § 226.14(c) are not subject to the rules or procedures of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(c) *Restrictions on use—(1) Prohibition on use in regulatory actions.* Federal, State, Local, and Tribal Government entities are prohibited from using information obtained solely through a CIRCIA Report submitted under this part or a response to a request for information issued under § 226.14(c) to regulate, including through an enforcement proceeding, the activities of the covered entity or the entity that made a ransom payment on the covered entity's behalf, except: (i) If the Federal, State, Local, or Tribal Government entity expressly allows the entity to meet its regulatory reporting obligations through submission of reports to CISA; or (ii) Consistent with Federal or State regulatory authority specifically relating to the prevention and mitigation of cybersecurity threats to information systems, a CIRCIA Report or response to a request for information issued under § 226.14(c) may inform the development or implementation of regulations relating to such systems.

(2) *Liability protection—(i) No cause of action.* No cause of action shall lie or be maintained in any court by any person or entity for the submission of a CIRCIA Report or a response to a request for information issued under § 226.14(c) and must be promptly dismissed by the court. This liability protection only applies to or affects litigation that is solely based on the submission of a CIRCIA Report or a response provided to a request for information issued under § 226.14(c).

(ii) *Evidentiary and discovery bar for reports.* CIRCIA Reports submitted under this part, responses provided to requests for information issued under § 226.14(c), or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting CIRCIA Reports or responses to requests for information issued under § 226.14(c), may not be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof. This bar does not create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting a CIRCIA Report under this part or a response to a request for information issued under § 226.14(c).

(iii) *Exception.* The liability protection provided in paragraph (c)(2)(i) of this section does not apply to an action taken by the Federal government pursuant to § 226.15.

(3) *Limitations on authorized uses.* Information provided to CISA in a CIRCIA Report or in a response to a request for information issued under § 226.14(c) may be disclosed to, retained by, and used by any Federal agency or department, component, officer, employee, or agent of the Federal Government, consistent with otherwise applicable provisions of Federal law, solely for the following purposes:

- (i) A cybersecurity purpose;
- (ii) The purpose of identifying a cybersecurity threat, including the source of the cybersecurity threat, or a security vulnerability;
- (iii) The purpose of responding to, or otherwise preventing or mitigating, a specific threat of:
 - (A) Death;
 - (B) Serious bodily harm; or
 - (C) Serious economic harm;
- (iv) The purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating a serious threat to a minor, including sexual exploitation and threats to physical safety; or
- (v) The purpose of preventing, investigating, disrupting, or prosecuting an offense:
 - (A) Arising out of events required to be reported in accordance with § 226.3;
 - (B) Described in 18 U.S.C. 1028 through 1030 relating to fraud and identity theft;
 - (C) Described in 18 U.S.C. chapter 37 relating to espionage and censorship; or

(D) Described in 18 U.S.C. 90 relating to protection of trade secrets.

§ 226.19 Procedures for protecting privacy and civil liberties.

(a) *In general.* The use of personal information received in CIRCIA Reports and in responses provided to requests for information issued under § 226.14(c) is subject to the procedures described in this section for protecting privacy and civil liberties. CISA will ensure that privacy controls and safeguards are in place at the point of receipt, retention, use, and dissemination of a CIRCIA Report. The requirements in this section do not apply to personal information submitted in response to a subpoena issued under § 226.14(d) or following Federal government action under §§ 226.15 through 226.17.

(b) *Instructions for submitting personal information.* A covered entity should only include the personal information requested by CISA in the web-based CIRCIA Incident Reporting Form or in the request for information and should exclude unnecessary personal information from CIRCIA Reports and responses to requests for information issued under § 226.14(c).

(c) *Assessment of personal information.* CISA will review each CIRCIA Report and response to request for information issued under § 226.14(c) to determine if the report contains personal information other than the information requested by CISA and whether the personal information is directly related to a cybersecurity threat. Personal information directly related to a cybersecurity threat includes personal information that is necessary to detect,

prevent, or mitigate a cybersecurity threat.

(1) If CISA determines the personal information is not directly related to a cybersecurity threat, nor necessary for contacting a covered entity or report submitter, CISA will delete the personal information from the CIRCIA Report or response to request for information. covered entity or report submitter contact information, including information of third parties submitting on behalf of an entity, will be safeguarded when retained and anonymized prior to sharing the report outside of the federal government unless CISA receives the consent of the individual for sharing personal information and the personal information can be shared without revealing the identity of the covered entity.

(2) If the personal information is determined to be directly related to a cybersecurity threat, CISA will retain the personal information and may share it consistent with § 226.18 of this part and the guidance described in paragraph (d) of this section.

(d) *Privacy and civil liberties guidance.* CISA will develop and make publicly available guidance relating to privacy and civil liberties to address the retention, use, and dissemination of personal information contained in Covered Cyber Incident Reports and Ransom Payment Reports by CISA. The guidance shall be consistent with the need to protect personal information from unauthorized use or disclosure, and to mitigate cybersecurity threats.

(1) One year after the publication of the guidance, CISA will review the

effectiveness of the guidance to ensure that it appropriately governs the retention, use, and dissemination of personal information pursuant to this part and will perform subsequent reviews periodically.

(2) The Chief Privacy Officer of CISA will complete an initial review of CISA's compliance with the privacy and civil liberties guidance approximately one year after the effective date of this part and subsequent periodic reviews not less frequently than every three years.

§ 226.20 Other procedural measures.

(a) *Penalty for false statements and representations.* Any person that knowingly and willfully makes a materially false or fraudulent statement or representation in connection with, or within, a CIRCIA Report, response to a request for information, or response to an administrative subpoena is subject to the penalties under 18 U.S.C. 1001.

(b) *Severability.* CISA intends the various provisions of this part to be severable from each other to the extent practicable, such that if a court of competent jurisdiction were to vacate or enjoin any one provision, the other provisions are intended to remain in effect unless they are dependent upon the vacated or enjoined provision.

Jennie M. Easterly,

Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

[FR Doc. 2024-06526 Filed 3-27-24; 8:45 am]

BILLING CODE 9110-G1-P



FEDERAL REGISTER

Vol. 89

Thursday,

No. 66

April 4, 2024

Part III

Department of Health and Human Services

Centers for Medicare & Medicaid Services

42 CFR Part 418

Medicare Program; FY 2025 Hospice Wage Index and Payment Rate Update, Hospice Conditions of Participation Updates, and Hospice Quality Reporting Program Requirements; Proposed Rule

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

42 CFR Part 418

[CMS–1810–P]

RIN 0938–AV29

Medicare Program; FY 2025 Hospice Wage Index and Payment Rate Update, Hospice Conditions of Participation Updates, and Hospice Quality Reporting Program Requirements

AGENCY: Centers for Medicare & Medicaid Services (CMS), Department of Health and Human Services (HHS).

ACTION: Proposed rule.

SUMMARY: This proposed rule would update the hospice wage index, payment rates, and aggregate cap amount for Fiscal Year (FY) 2025. This rule proposes changes to the Hospice Quality Reporting Program. This rule also proposes to adopt the most recent Office of Management and Budget statistical area delineations, which would change the hospice wage index. This rule proposes to clarify current policy related to the “election statement” and the “notice of election”, as well as to add clarifying language regarding hospice certification. Finally, this rulemaking solicits comments regarding potential implementation of a separate payment mechanism to account for high intensity palliative care services.

DATES: To be assured consideration, comments must be received at one of the addresses provided below, no later than May 28, 2024.

ADDRESSES: In commenting, refer to file code CMS–1810–P.

Comments, including mass comment submissions, must be submitted in one of the following three ways (choose *only one* of the ways listed):

1. *Electronically.* You may submit electronic comments on this regulation to <http://www.regulations.gov>. Follow the “Submit a comment” instructions.

2. *By regular mail.* You may mail written comments to the following address ONLY: Centers for Medicare & Medicaid Services, Department of Health and Human Services, Attention: CMS–1810–P, P.O. Box 8010, Baltimore, MD 21244–1850.

Please allow sufficient time for mailed comments to be received before the close of the comment period.

3. *By express or overnight mail.* You may send written comments to the following address ONLY: Centers for

Medicare & Medicaid Services, Department of Health and Human Services, Attention: CMS–1810–P, Mail Stop C4–26–05, 7500 Security Boulevard, Baltimore, MD 21244–1850.

For information on viewing public comments, see the beginning of the **SUPPLEMENTARY INFORMATION** section.

FOR FURTHER INFORMATION CONTACT:

For general questions about hospice payment policy, send your inquiry via email to: hospicpolicy@cms.hhs.gov.

For questions regarding the CAHPS® Hospice Survey, contact Lauren Fuentes at (410) 786–2290.

For questions regarding the hospice conditions of participation (CoPs), contact Mary Rossi-Coajou at (410) 786–6051.

For questions regarding the hospice quality reporting program, contact Jermama Keys at (410) 786–7778.

SUPPLEMENTARY INFORMATION:

Inspection of Public Comments: All comments received before the close of the comment period are available for viewing by the public, including any personally identifiable or confidential business information that is included in a comment. We post all comments received before the close of the comment period on the following website as soon as possible after they have been received: <http://www.regulations.gov>. Follow the search instructions on that website to view public comments. CMS will not post on *Regulations.gov* public comments that make threats to individuals or institutions or suggest that the individual will take actions to harm the individual. CMS continues to encourage individuals not to submit duplicative comments. We will post acceptable comments from multiple unique commenters even if the content is identical or nearly identical to other comments.

Plain Language Summary: In accordance with 5 U.S.C. 553(b)(4), a plain language summary of this proposed rule may be found at <https://www.regulations.gov/>.

I. Executive Summary

A. Purpose

This proposed rule would update the hospice wage index, payment rates, and cap amount for Fiscal Year (FY) 2025 as required under section 1814(i) of the Social Security Act (the Act).

This rule also proposes to adopt the most recent Office of Management and Budget (OMB) statistical area delineations based on data collected during the 2020 Decennial Census, which would result in changes to the hospice wage index. In addition, this

rule proposes reorganization of the regulations to clarify current policy related to the “election statement” and the “notice of election (NOE),” as well as to add clarifying language regarding who can certify terminal illness. This rulemaking solicits comments on a potential policy to account for the increased hospice costs of providing high intensity palliative care services. In past rules, we have presented data regarding important hospice utilization trends. This year, and in subsequent years, the monitoring section will be removed from the rulemaking and placed on the CMS hospice center web page, which can be found at <https://www.cms.gov/medicare/payment/fee-for-service-providers/hospice>.

This rule also proposes that Hospice Quality Reporting Program (HQRP) measures be collected through a new collection instrument, the Hospice Outcomes and Patient Evaluation (HOPE); this rule also proposes two HOPE-based measures and lays out the planned trajectory for further development of this instrument; requests information regarding potential social determinants of health (SDOH) elements and provides updates on Health Equity, future quality measures (QMs), and public reporting requirements. Finally, this rule also proposes changes to the Hospice Consumer Assessment of Healthcare Providers and Systems (Hospice CAHPS) Survey.

B. Summary of the Major Provisions

Section III.A.1 of this proposed rule proposes updates to the hospice wage index and makes the application of the updated wage data budget neutral for all four levels of hospice care.

Section III.A.2 of this proposed rule proposes to adopt the new OMB labor market delineations from the July 21, 2023, OMB Bulletin No. 23–01 based on data collected from the 2020 Decennial Census.

Section III.A.3 of this proposed rule includes the proposed FY 2025 hospice payment update percentage of 2.6 percent.

Section III.A.4 of this proposed rule proposes updates to the hospice payment rates.

Section III.A.5 of this proposed rule includes the proposed update to the hospice cap amount for FY 2025 by the hospice payment update percentage of 2.6 percent.

In section III.B of this proposed rule, we propose clarifying regulation text changes, with no change to current policy. This includes reorganizing the regulations to clearly identify the distinction between the “election

statement” and the “notice of election,” as well as including clarifying text changes that align payment regulations and Conditions of Participation (CoPs) regarding who may certify terminal illness and determine admission to hospice care.

In section III.C of this proposed rule, we include a Request for Information (RFI) on a potential policy to account for higher hospice costs involved in the provision of high intensity palliative care treatments.

Finally, in section III.D of this rule proposed rule, we propose HOPE-based process measures; the HOPE instrument; discuss updates to potential future quality measures; and propose changes to the CAHPS® Hospice Survey.

C. Summary of Impacts

The overall economic impact of this proposed rule is estimated to be \$705 million in increased payments to hospices in FY 2025.

II. Background

A. Hospice Care

Hospice care is a comprehensive, holistic approach to treatment that recognizes the impending death of a terminally ill individual and warrants a change in the focus from curative care to palliative care for relief of pain and for symptom management. Medicare regulations define “palliative care” as patient and family centered care that optimizes quality of life by anticipating, preventing, and treating suffering. Palliative care throughout the continuum of illness involves addressing physical, intellectual, emotional, social, and spiritual needs and to facilitate patient autonomy, access to information, and choice (42 CFR 418.3). Palliative care is at the core of hospice philosophy and care practices and is a critical component of the Medicare hospice benefit.

The goal of hospice care is to help terminally ill individuals continue life with minimal disruption to normal activities while remaining primarily in the home environment. A hospice uses an interdisciplinary approach to deliver medical, nursing, social, psychological, emotional, and spiritual services through a collaboration of professionals and other caregivers, with the goal of making the beneficiary as physically and emotionally comfortable as possible. Hospice is compassionate beneficiary and family/caregiver-centered care for those who are terminally ill.

As referenced in our regulations at § 418.22(b)(1), to be eligible for Medicare hospice services, the patient’s

attending physician (if any) and the hospice medical director must certify that the individual is “terminally ill,” as defined in section 1861(dd)(3)(A) of the Act and our regulations at § 418.3; that is, the individual has a medical prognosis that his or her life expectancy is 6 months or less if the illness runs its normal course. The regulations at § 418.22(b)(2) require that clinical information and other documentation that support the medical prognosis accompany the certification and be filed in the medical record with it. The regulations at § 418.22(b)(3) require that the certification and recertification forms include a brief narrative explanation of the clinical findings that support a life expectancy of 6 months or less.

Under the Medicare hospice benefit, the election of hospice care is a patient choice and once a terminally ill patient elects to receive hospice care, a hospice interdisciplinary group is essential in the seamless provision of primarily home-based services. The hospice interdisciplinary group works with the beneficiary, family, and caregivers to develop a coordinated, comprehensive care plan; reduce unnecessary diagnostics or ineffective therapies; and maintain ongoing communication with individuals and their families about changes in their condition. The beneficiary’s care plan will shift over time to meet the changing needs of the individual, family, and caregiver(s) as the individual approaches the end of life.

If, in the judgment of the hospice interdisciplinary group, which includes the hospice physician, the patient’s symptoms cannot be effectively managed at home, then the patient is eligible for general inpatient care (GIP), a more medically intense level of care. GIP must be provided in a Medicare-certified hospice freestanding facility, skilled nursing facility, or hospital. GIP is provided to ensure that any new or worsening symptoms are intensively addressed so that the beneficiary can return to their home and continue to receive routine home care (RHC). Limited, short-term, intermittent, inpatient respite care (IRC) is also available because of the absence or need for relief of the family or other caregivers. Additionally, an individual can receive continuous home care (CHC) during a period of crisis in which an individual requires continuous care to achieve palliation or management of acute medical symptoms so that the individual can remain at home. CHC may be covered for as much as 24 hours a day, and these periods must be predominantly nursing care, in

accordance with the regulations at § 418.204. A minimum of 8 hours of nursing care or nursing and aide care must be furnished on a particular day to qualify for the CHC rate (§ 418.302(e)(4)).

Hospices covered by this proposed rule must comply with applicable civil rights laws, including section 1557 of the Affordable Care Act, section 504 of the Rehabilitation Act of 1973 and the Americans with Disabilities Act, which require covered programs to take appropriate steps to ensure effective communication with individuals with disabilities and companions with disabilities, including the provisions of auxiliary aids and services when necessary for effective communication.¹ Further information may be found at: <https://www.hhs.gov/civil-rights/index.html>.

Title VI of the Civil Rights Act of 1964 prohibits discrimination on the basis of race, color or national origin in federally assisted programs or activities. The Office for Civil Rights (OCR) interprets this to require that recipients of Federal financial assistance take reasonable steps to provide meaningful access to their programs or activities to individuals with limited English proficiency (LEP).² Similarly, Section 1557’s implementing regulation requires covered entities to take reasonable steps to provide meaningful access to LEP individuals in federally funded health programs and activities (45 CFR 92.101(a)). Meaningful access may require the provision of interpreter services and translated materials (45 CFR 92.101(a)(2)).

B. Services Covered by the Medicare Hospice Benefit

Coverage under the Medicare hospice benefit requires that hospice services must be reasonable and necessary for the palliation and management of the terminal illness and related conditions. Section 1861(dd)(1) of the Act establishes the services that are to be rendered by a Medicare-certified hospice program. These covered services include: nursing care; physical therapy; occupational therapy; speech-

¹ Hospices receiving Medicare Part A funds or other Federal financial assistance from the Department are also subject to additional Federal civil rights laws, including the Age Discrimination Act, and are subject to conscience and religious freedom laws where applicable.

² HHS OCR, *Guidance to Federal Financial Assistance Recipients Regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient Persons*, 68 FR 47311 (Aug. 8, 2003), <https://www.hhs.gov/civil-rights/for-individuals/special-topics/limited-english-proficiency/guidance-federal-financial-assistance-recipients-title-vi/index.html>.

language pathology therapy; medical social services; home health aide services (called hospice aide services); physician services; homemaker services; medical supplies (including drugs and biologicals); medical appliances; counseling services (including dietary counseling); short-term inpatient care in a hospital, nursing facility, or hospice inpatient facility (including both respite care and care and procedures necessary for pain control and acute or chronic symptom management); continuous home care during periods of crisis, and only as necessary, to maintain the terminally ill individual at home; and any other item or service which is specified in the plan of care and for which payment may otherwise be made under Medicare, in accordance with Title XVIII of the Act.

Section 1814(a)(7)(B) of the Act requires that a written plan for providing hospice care to a beneficiary, who is a hospice patient, be established before care is provided by, or under arrangements made by, the hospice program; and that the written plan be periodically reviewed by the beneficiary's attending physician (if any), the hospice medical director, and an interdisciplinary group (section 1861(dd)(2)(B) of the Act). The services offered under the Medicare hospice benefit must be available to beneficiaries as needed, 24 hours a day, 7 days a week (section 1861(dd)(2)(A)(i) of the Act).

Upon the implementation of the hospice benefit, Congress also expected hospices to continue to use volunteer services, although Medicare does not pay for these volunteer services (section 1861(dd)(2)(E) of the Act). As stated in the Health Care Financing Administration's (now Centers for Medicare & Medicaid Services (CMS)) proposed rule "Medicare Program; Hospice Care (48 FR 38149), the hospice must have an interdisciplinary group composed of paid hospice employees as well as hospice volunteers, and that "the hospice benefit and the resulting Medicare reimbursement is not intended to diminish the voluntary spirit of hospices." This expectation supports the hospice philosophy of community based, holistic, comprehensive, and compassionate end of life care.

C. Medicare Payment for Hospice Care

Sections 1812(d), 1813(a)(4), 1814(a)(7), 1814(i), and 1861(dd) of the Act, and the regulations in 42 CFR part 418, establish eligibility requirements, payment standards and procedures; define covered services; and delineate the conditions a hospice must meet to

be approved for participation in the Medicare program. Part 418, subpart G, provides for a per diem payment based on one of four prospectively determined rate categories of hospice care (RHC, CHC, IRC, and GIP), based on each day a qualified Medicare beneficiary is under hospice care (once the individual has elected the benefit). This per diem payment is meant to cover all hospice services and items needed to manage the beneficiary's care, as required by section 1861(dd)(1) of the Act.

While payment made to hospices is to cover all items, services, and drugs for the palliation and management of the terminal illness and related conditions, Federal funds cannot be used for prohibited activities, even in the context of a per diem payment. For example, hospices are prohibited from playing a role in medical aid in dying (MAID) where such practices have been legalized in certain states. The Assisted Suicide Funding Restriction Act of 1997 (Pub. L. 105-12, April 30, 1997) prohibits the use of Federal funds to provide or pay for any health care item or service or health benefit coverage for the purpose of causing, or assisting to cause, the death of any individual including "mercy killing, euthanasia, or assisted suicide." However, the prohibition does not pertain to the provision of an item or service for the purpose of alleviating pain or discomfort, even if such use may increase the risk of death, so long as the item or service is not furnished for the specific purpose of causing or accelerating death.

The Medicare hospice benefit has been revised and refined since its implementation after various Acts of Congress and Medicare rules. For a historical list of changes and regulatory actions, we refer readers to the background section of previous Hospice Wage Index and Payment Rate Update rules.³

III. Provisions of the Proposed Rule

A. Proposed FY 2025 Hospice Wage Index and Rate Update

1. Proposed FY 2025 Hospice Wage Index

The hospice wage index is used to adjust payment rates for hospices under the Medicare program to reflect local differences in area wage levels, based on the location where services are furnished. Our regulations at § 418.306(c) require each labor market to

be established using the most current hospital wage data available, including any changes made by the Office of Management and Budget (OMB) to Metropolitan Statistical Area (MSA) definitions.

In general, OMB issues major revisions to statistical areas every 10 years, based on the results of the decennial census. However, OMB occasionally issues minor updates and revisions to statistical areas in the years between the decennial censuses. On September 14, 2018, OMB issued OMB Bulletin No. 18-04, which superseded the April 10, 2018 OMB Bulletin No. 18-03. OMB Bulletin No. 18-04 made revisions to the delineations of Metropolitan Statistical Areas (MSAs), Micropolitan Statistical Areas, and Combined Statistical Areas, and guidance on uses of the delineations in these areas. This bulletin provided the delineations of all MSAs, Metropolitan Divisions, Micropolitan Statistical Areas, Combined Statistical Areas, and New England City and Town Areas in the United States and Puerto Rico based on the standards published on June 28, 2010, in the **Federal Register** (75 FR 37246 through 37252), and Census Bureau data. A copy of the September 14, 2018 bulletin is available online at: <https://www.whitehouse.gov/wp-content/uploads/2018/09/Bulletin-18-04.pdf>. In the FY 2021 Hospice Wage Index final rule (85 FR 47080), we finalized our proposal to adopt the revised OMB delineations from the September 14, 2018 OMB Bulletin 18-04 with a 5-percent cap on wage index decreases, where the estimated reduction in a geographic area's wage index would be capped at 5-percent in FY 2021 and no cap would be applied to wage index decreases for the second year (FY 2022). On March 6, 2020, OMB issued Bulletin No. 20-01, which provided updates to and superseded OMB Bulletin No. 18-04 that was issued on September 14, 2018. The attachments to OMB Bulletin No. 20-01 provided detailed information on the update to statistical areas since September 14, 2018, and were based on the application of the 2010 Standards for Delineating Metropolitan and Micropolitan Statistical Areas to Census Bureau population estimates for July 1, 2017 and July 1, 2018. (For a copy of this bulletin, we refer readers to the following website: <https://www.whitehouse.gov/wp-content/uploads/2020/03/Bulletin-20-01.pdf>.) In OMB Bulletin No. 20-01, OMB announced one new Micropolitan Statistical Area, one new component of an existing Combined Statistical Area

³ Hospice Regulations and Notices. <https://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/Hospice/Hospice-Regulations-and-Notices>.

(CSA), and changes to New England City and Town Area (NECTA) delineations. In the FY 2021 Hospice Wage Index final rule (85 FR 47070) we stated that if appropriate, we would propose any updates from OMB Bulletin No. 20–01 in future rulemaking. After reviewing OMB Bulletin No. 20–01, we determined that the changes in Bulletin 20–01 encompassed delineation changes that would not affect the Medicare wage index for FY 2022. Specifically, the updates consisted of changes to NECTA delineations and the redesignation of a single rural county into a newly created Micropolitan Statistical Area. The Medicare wage index does not utilize NECTA definitions, and, as most recently discussed in the FY 2021 Hospice Wage Index final rule (85 FR 47070), we include hospitals located in Micropolitan Statistical areas in each State's rural wage index.

As described in the August 8, 1997 Hospice Wage Index final rule (62 FR 42860), the pre-floor and pre-reclassified hospital wage index is used as the raw wage index for the hospice benefit. These raw wage index values are subject to application of the hospice floor to compute the hospice wage index used to determine payments to hospices. As previously discussed, the pre-floor, pre-reclassified hospital wage index values below 0.8 will be further adjusted by a 15 percent increase subject to a maximum wage index value of 0.8. For example, if County A has a pre-floor, pre-reclassified hospital wage index value of 0.3994, we would multiply 0.3994 by 1.15, which equals 0.4593. Since 0.4593 is not greater than 0.8, then County A's hospice wage index would be 0.4593. In another example, if County B has a pre-floor, pre-reclassified hospital wage index value of 0.7440, we would multiply 0.7440 by 1.15, which equals 0.8556. Because 0.8556 is greater than 0.8, County B's hospice wage index would be 0.8.

In the FY 2023 Hospice Wage Index final rule (87 FR 45673), we finalized for FY 2023 and subsequent years, the application of a permanent 5-percent cap on any decrease to a geographic area's wage index from its wage index in the prior year, regardless of the circumstances causing the decline, so that a geographic area's wage index would not be less than 95 percent of its wage index calculated in the prior FY. When calculating the 5-percent cap on wage index decreases we start with the current fiscal year's pre-floor, pre-reclassification hospital wage index value for a core-based statistical area (CBSA) or statewide rural area and if that wage index value is below 0.8000,

we apply the hospice floor as discussed above. Next, we compare the current fiscal year's wage index value after the application of the hospice floor to the final wage index value from the previous fiscal year. If the current fiscal year's wage index value is less than 95 percent of the previous year's wage index value, the 5-percent cap on wage index decreases would be applied and the final wage index value would be set equal to 95 percent of the previous fiscal year's wage index value. If the 5-percent cap is applied in one fiscal year, then in the subsequent fiscal year, that year's pre-floor, pre-reclassification hospital wage index would be used as the starting wage index value and adjusted by the hospice floor. The hospice floor adjusted wage index value would be compared to the previous fiscal year's wage index which had the 5-percent cap applied. If the hospice floor adjusted wage index value for that fiscal year is less than 95 percent of the capped wage index from the previous year, then the 5-percent cap would be applied again, and the final wage index value would be 95 percent of the capped wage index from the previous fiscal year. Using the example from above, if County A has a pre-floor, pre-reclassified hospital wage index value of 0.3994, we would multiply 0.3994 by 1.15, which equals 0.4593. If County A had a wage index value of 0.6200 in the previous fiscal, then we would compare 0.4593 to the previous fiscal year's wage index value. Since 0.4593 is less than 95 percent of 0.6200, then County A's hospice wage index would be 0.5890, which is equal to 95-percent of the previous fiscal year's wage index value of 0.6200. In the next fiscal year, the updated wage index value would be compared to the wage index value of 0.5890.

Previously, this methodology was applied to all the counties that make up the CBSA or rural area. However, as discussed in section III.A.2.f., if we adopt the revised OMB delineations this methodology would also be applied to individual counties.

In the FY 2020 Hospice Wage Index final rule (84 FR 38484), we finalized the proposal to use the current FY's hospital wage index data to calculate the hospice wage index values. For FY 2025, we are proposing that the proposed hospice wage index would be based on the FY 2025 hospital pre-floor, pre-reclassified wage index for hospital cost reporting periods beginning on or after October 1, 2020 and before October 1, 2021 (FY 2021 cost report data). The proposed FY 2025 hospice wage index would not take into account any geographic reclassification of hospitals, including those in accordance with

section 1886(d)(8)(B) or 1886(d)(10) of the Act. The regulations that govern hospice payment do not provide a mechanism for allowing hospices to seek geographic reclassification or to utilize the rural floor provisions that exist for IPPS hospitals. The reclassification provision found in section 1886(d)(10) of the Act is specific to hospitals. Section 4410(a) of the Balanced Budget Act of 1997 (Pub. L. 105–33) provides that the area wage index applicable to any hospital that is located in an urban area of a State may not be less than the area wage index applicable to hospitals located in rural areas in that State. This rural floor provision is also specific to hospitals. Because the reclassification and the hospital rural floor policies apply to hospitals only, and not to hospices, we continue to believe the use of the pre-floor and pre-reclassified hospital wage index results is the most appropriate adjustment to the labor portion of the hospice payment rates. This position is longstanding and consistent with other Medicare payment systems, for example, skilled nursing facility prospective payment system (SNF PPS), inpatient rehabilitation facility prospective payment system (IRF PPS), and home health prospective payment system (HH PPS). However, the hospice wage index does include the hospice floor, which is applicable to all CBSAs, both rural and urban. The hospice floor adjusts pre-floor, pre-reclassified hospital wage index values below 0.8 by a 15 percent increase subject to a maximum wage index value of 0.8. The proposed FY 2025 hospice wage index would also include the 5-percent cap on wage index decreases. The appropriate wage index value would be applied to the labor portion of the hospice payment rate based on the geographic area in which the beneficiary resides when receiving RHC or CHC. The appropriate wage index value is applied to the labor portion of the payment rate based on the geographic location of the facility for beneficiaries receiving GIP or IRC.

There exist some geographic areas where there are no hospitals, and thus, no hospital wage data on which to base the calculation of the hospice wage index. In the FY 2006 Hospice Wage Index final rule (70 FR 45135), we adopted the policy that, for urban labor markets without a hospital from which hospital wage index data could be derived, all of the CBSAs within the State would be used to calculate a statewide urban average pre-floor, pre-reclassified hospital wage index value to use as a reasonable proxy for these

areas. For FY 2025, the only CBSA without a hospital from which hospital wage data can be derived is 25980, Hinesville-Fort Stewart, Georgia. The FY 2025 proposed wage index value for Hinesville-Fort Stewart, Georgia is 0.8726.

In the FY 2008 Hospice Wage Index final rule (72 FR 50217 through 50218), we implemented a methodology to update the hospice wage index for rural areas without hospital wage data. In cases where there was a rural area

without rural hospital wage data, we use the average pre-floor, pre-reclassified hospital wage index data from all contiguous CBSAs, to represent a reasonable proxy for the rural area. The term “contiguous” means sharing a border (72 FR 50217). For FY 2025, as part of our proposal to adopt the revised OMB delineations discussed further in section III.A.2, we are proposing that rural North Dakota would now become a rural area without a hospital from which hospital wage data can be

devised. Therefore, to calculate the wage index for rural area 99935, North Dakota, we are proposing to use as a proxy, the average pre-floor, pre-reclassified hospital wage data (updated by the hospice floor) from the contiguous CBSAs: CBSA 13900-Bismarck, ND, CBSA 22020-Fargo, ND-MN, CBSA 24220-Grand Forks, ND-MN and CBSA 33500, Minot, ND, which results in a proposed FY 2025 hospice wage index of 0.8446 for rural North Dakota.

Table 1: Wage Index For Rural North Dakota.

CBSA Code	CBSA Name	Hospice Wage Index
13900	Bismarck, ND	0.9020
22020	Fargo, ND-MN	0.8763
24220	Grand Forks, ND-MN	0.8000
33500	Minot, ND	0.8000
Proposed FY 2025 Hospice Wage Index		0.8446

Note: CBSA 24220 Grand Forks, ND-MN and CBSA 33500 Minot, ND are adjusted by the hospice floor.

Previously, the only rural area without a hospital from which hospital wage data could be derived was in Puerto Rico. However, for rural Puerto Rico, we did not apply this methodology due to the distinct economic circumstances that exist there (for example, due to the close proximity of almost all of Puerto Rico’s various urban areas to non-urban areas, this methodology would produce a wage index for rural Puerto Rico that is higher than that in half of its urban areas); instead, we used the most recent wage index previously available for that area which was 0.4047, subsequently adjusted by the hospice floor for an adjusted wage index value of 0.4654. For FY 2025, as part of our proposal to adopt the revised OMB delineations discussed further in section III.A.2.c. below, there would now be a hospital in rural Puerto Rico from which hospital wage data can be derived. Therefore, we are proposing that the wage index for rural Puerto Rico would now be based on the hospital wage data for the area instead of the previously available pre-hospice floor wage index of 0.4047, which equaled an adjusted wage index value of 0.4654. The FY 2025 proposed pre-hospice floor unadjusted wage index for rural Puerto Rico would be 0.2520, and is subsequently adjusted by the hospice floor to equal 0.2898. Because 0.2898 is more than a 5-percent

decline in the FY 2024 wage index, the adjusted FY 2025 wage index with the 5-percent cap applied would equal 0.95 multiplied by 0.4654 (that is, the FY 2024 wage index with floor), which results in a proposed wage index of 0.4421.

Finally, we are proposing that for FY 2025, if the adoption of the revised OMB delineations is finalized that Delaware, which was previously an all-urban State, would now have one rural area with a hospital from which hospital wage data can be derived. The proposed FY 2025 wage index for rural area 99908 Delaware would be 1.0429.

2. Proposed Implementation of New Labor Market Delineations

On July 21, 2023, OMB issued Bulletin No. 23–01, which updates and supersedes OMB Bulletin No. 20–01, issued on March 6, 2020. OMB Bulletin No. 23–01 establishes revised delineations for the MSAs, Micropolitan Statistical Areas, Combined Statistical Areas, and Metropolitan Divisions, collectively referred to as Core Based Statistical Areas (CBSAs). According to OMB, the delineations reflect the 2020 Standards for Delineating Core Based Statistical Areas (CBSAs) (the “2020 Standards”), which appeared in the **Federal Register** (86 FR 37770 through 37778) on July 16, 2021, and application of those standards to Census Bureau

population and journey-to-work data (for example, 2020 Decennial Census, American Community Survey, and Census Population Estimates Program data). A copy of OMB Bulletin No. 23–01 is available online at: <https://www.whitehouse.gov/wp-content/uploads/2023/07/OMB-Bulletin-23-01.pdf>.

The July 21, 2023 OMB Bulletin No. 23–01 contains a number of significant changes. For example, there are new CBSAs, urban counties that have become rural, rural counties that have become urban, and existing CBSAs that have been split apart. We believe it is important for the hospice wage index to use the latest OMB delineations available in order to maintain a more accurate and up-to-date payment system that reflects the reality of population shifts and labor market conditions. We further believe that using the most current OMB delineations would increase the integrity of the hospice wage index by creating a more accurate representation of geographic variation in wage levels. We are proposing to implement the new OMB delineations as described in the July 21, 2023 OMB Bulletin No. 23–01 for the hospice wage index effective beginning in FY 2025.

a. Micropolitan Statistical Areas

As discussed in the FY 2006 Hospice Wage Index and Payment Rate Update

proposed rule (70 FR 22397) and final rule (70 FR 45132), we considered how to use the Micropolitan Statistical Area definitions in the calculation of the wage index. Previously, OMB defined a “Micropolitan Statistical Area” as a “CBSA” “associated with at least one urban cluster that has a population of at least 10,000, but less than 50,000” (75 FR 37252). We refer to these as Micropolitan Areas. After extensive impact analysis, consistent with the treatment of these areas under the Inpatient Prospective Payment System (IPPS) as discussed in the FY 2005 IPPS final rule (69 FR 49029), we determined the best course of action would be to treat Micropolitan Areas as “rural” and include them in the calculation of each State’s Hospice rural wage index (70 FR 22397 and 70 FR 45132). Thus, the hospice statewide rural wage index has been determined using IPPS hospital data from hospitals located in non-MSAs. In the FY 2021 Hospice final rule (85 FR 47074, 47080), we finalized a policy to continue to treat Micropolitan Areas as “rural” and to include Micropolitan Areas in the calculation of each State’s rural wage index.

The OMB “2020 Standards” continues to define a “Micropolitan Statistical Area” as a CBSA with at least

one Urban Area that has a population of at least 10,000, but less than 50,000. The Micropolitan Statistical Area comprises the central county or counties containing the core, plus adjacent outlying counties having a high degree of social and economic integration with the central county or counties as measured through commuting. (86 FR 37778). Overall, there are the same number of Micropolitan Areas (542) under the new OMB delineations based on the 2020 Census as there were using the 2010 Census. We note, however, that a number of urban counties have switched status and have joined or became Micropolitan Areas, and some counties that once were part of a Micropolitan Area, and thus were treated as rural, have become urban based on the 2020 Decennial Census data. We believe that the best course of action would be to continue our established policy and include Micropolitan Areas in each State’s rural wage index as these areas continue to be defined as having relatively small urban cores (populations of 10,000 to 49,999). Therefore, in conjunction with our proposal to implement the new OMB labor market delineations beginning in FY 2025, and consistent with the treatment of Micropolitan Areas under

the IPPS, we are also proposing to continue to treat Micropolitan Areas as “rural” and to include Micropolitan Areas in the calculation of each State’s rural wage index.

b. Change to County-Equivalents in the State of Connecticut

In a June 6, 2022 Notice (87 FR 34235–34240), the Census Bureau announced that it was implementing the State of Connecticut’s request to replace the eight counties in the State with nine new “Planning Regions.” Planning regions are included in OMB Bulletin No. 23–01 and now serve as county-equivalents within the CBSA system. We have evaluated the change and are proposing to adopt the planning regions as county equivalents for wage index purposes. We believe it is necessary to adopt this migration from counties to planning region county-equivalents in order to maintain consistency with our established policy of adopting the most recent OMB updates. We are providing the following crosswalk in Table 2 for counties located in Connecticut with the current and proposed FIPS county and county-equivalent codes and CBSA assignments.

BILLING CODE 4120-01-P

TABLE 2: Crosswalk of Connecticut County Equivalents

FIPS County Code	County	Old CBSA or non-urban area	New FIPS County Code	FY 2025 Planning Region	New CBSA or non-urban area
09001	FAIRFIELD	14860	09190	WESTERN CONNECTICUT	14860
09001	FAIRFIELD	14860	09120	GREATER BRIDGEPORT	14860
09003	HARTFORD	25540	09110	CAPITOL	25540
09005	LITCHFIELD	99907	09160	NORTHWEST HILLS	99907
09007	MIDDLESEX	25540	09130	LOWER CONNECTICUT RIVER VALLEY	25540
09009	NEW HAVEN	35300	09140	NAUGATUCK VALLEY	47930
09009	NEW HAVEN	35300	09170	SOUTH CENTRAL CONNECTICUT	35300
09011	NEW LONDON	35980	09180	SOUTHEASTERN CONNECTICUT	35980
09013	TOLLAND	25540	09110	CAPITOL	25540
09015	WINDHAM	49340	09150	NORTHEASTERN CONNECTICUT	99907

c. Urban Counties That Would Become Rural

Under the revised OMB statistical area delineations (based upon OMB

Bulletin No. 23–01), a total of 53 counties (and county equivalents) that are currently considered urban would be considered rural beginning in FY

2025. Table 3 lists the 53 counties that would become rural if we adopt as final our proposal to implement the revised OMB delineations.

TABLE 3: Urban Counties That Would Change to Rural Status

FIPS County Code	County Name	State	Current CBSA	Current CBSA Name
01129	WASHINGTON	AL	33660	Mobile, AL
05025	CLEVELAND	AR	38220	Pine Bluff, AR
05047	FRANKLIN	AR	22900	Fort Smith, AR-OK
05069	JEFFERSON	AR	38220	Pine Bluff, AR
05079	LINCOLN	AR	38220	Pine Bluff, AR
10005	SUSSEX	DE	41540	Salisbury, MD-DE
13171	LAMAR	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA
16077	POWER	ID	38540	Pocatello, ID
17057	FULTON	IL	37900	Peoria, IL
17077	JACKSON	IL	16060	Carbondale-Marion, IL
17087	JOHNSON	IL	16060	Carbondale-Marion, IL
17183	VERMILION	IL	19180	Danville, IL
17199	WILLIAMSON	IL	16060	Carbondale-Marion, IL
18121	PARKE	IN	45460	Terre Haute, IN
18133	PUTNAM	IN	26900	Indianapolis-Carmel-Anderson, IN
18161	UNION	IN	17140	Cincinnati, OH-KY-IN
21091	HANCOCK	KY	36980	Owensboro, KY
21101	HENDERSON	KY	21780	Evansville, IN-KY
22045	IBERIA	LA	29180	Lafayette, LA
24001	ALLEGANY	MD	19060	Cumberland, MD-WV
24047	WORCESTER	MD	41540	Salisbury, MD-DE
25011	FRANKLIN	MA	44140	Springfield, MA
26155	SHIAWASSEE	MI	29620	Lansing-East Lansing, MI
27075	LAKE	MN	20260	Duluth, MN-WI
28031	COVINGTON	MS	25620	Hattiesburg, MS
31051	DIXON	NE	43580	Sioux City, IA-NE-SD
36123	YATES	NY	40380	Rochester, NY
37049	CRAVEN	NC	35100	New Bern, NC
37077	GRANVILLE	NC	20500	Durham-Chapel Hill, NC
37085	HARNETT	NC	22180	Fayetteville, NC
37087	HAYWOOD	NC	11700	Asheville, NC
37103	JONES	NC	35100	New Bern, NC
37137	PAMLICO	NC	35100	New Bern, NC
42037	COLUMBIA	PA	14100	Bloomsburg-Berwick, PA
42085	MERCER	PA	49660	Youngstown-Warren-Boardman, OH-PA
42089	MONROE	PA	20700	East Stroudsburg, PA
42093	MONTOUR	PA	14100	Bloomsburg-Berwick, PA
42103	PIKE	PA	35084	Newark, NJ-PA
45027	CLARENDON	SC	44940	Sumter, SC
48431	STERLING	TX	41660	San Angelo, TX
49003	BOX ELDER	UT	36260	Ogden-Clearfield, UT
51113	MADISON	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV

FIPS County Code	County Name	State	Current CBSA	Current CBSA Name
51175	SOUTHAMPTON	VA	47260	Virginia Beach-Norfolk-Newport News, VA-NC
51620	FRANKLIN CITY	VA	47260	Virginia Beach-Norfolk-Newport News, VA-NC
54035	JACKSON	WV	16620	Charleston, WV
54043	LINCOLN	WV	16620	Charleston, WV
54057	MINERAL	WV	19060	Cumberland, MD-WV
55069	LINCOLN	WI	48140	Wausau-Weston, WI
72001	ADJUNTAS	PR	38660	Ponce, PR
72055	GUANICA	PR	49500	Yauco, PR
72081	LARES	PR	10380	Aguadilla-Isabela, PR
72083	LAS MARIAS	PR	32420	Mayagüez, PR
72141	UTUADO	PR	10380	Aguadilla-Isabela, PR

d. Rural Counties That Would Become Urban

Under the revised OMB statistical area delineations (based upon OMB

Bulletin No. 23–01), a total of 54 counties (and county equivalents) that are currently located in rural areas would be considered located in urban areas under the revised OMB

delineations beginning in FY 2025. Table 4 lists the 54 counties that would be urban if we adopt as final our proposal to implement the revised OMB delineations.

TABLE 4: Rural Counties That Would Change to Urban Status

FIPS County Code	County Name	State	Proposed FY 2025 CBSA	Proposed FY 2025 CBSA Name
01087	MACON	AL	12220	Auburn-Opelika, AL
01127	WALKER	AL	13820	Birmingham, AL
12133	WASHINGTON	FL	37460	Panama City-Panama City Beach, FL
13187	LUMPKIN	GA	12054	Atlanta-Sandy Springs-Roswell, GA
15005	KALAWAO	HI	27980	Kahului-Wailuku, HI
17053	FORD	IL	16580	Champaign-Urbana, IL
17127	MASSAC	IL	37140	Paducah, KY-IL
18159	TIPTON	IN	26900	Indianapolis-Carmel-Greenwood, IN
18179	WELLS	IN	23060	Fort Wayne, IN
20021	CHEROKEE	KS	27900	Joplin, MO-KS
21007	BALLARD	KY	37140	Paducah, KY-IL
21039	CARLISLE	KY	37140	Paducah, KY-IL
21127	LAWRENCE	KY	26580	Huntington-Ashland, WV-KY-OH
21139	LIVINGSTON	KY	37140	Paducah, KY-IL
21145	MC CRACKEN	KY	37140	Paducah, KY-IL
21179	NELSON	KY	31140	Louisville/Jefferson County, KY-IN
22053	JEFFERSON DAVIS	LA	29340	Lake Charles, LA
22083	RICHLAND	LA	33740	Monroe, LA
26015	BARRY	MI	24340	Grand Rapids-Wyoming-Kentwood, MI
26019	BENZIE	MI	45900	Traverse City, MI
26055	GRAND TRAVERSE	MI	45900	Traverse City, MI
26079	KALKASKA	MI	45900	Traverse City, MI
26089	LEELANAU	MI	45900	Traverse City, MI
27133	ROCK	MN	43620	Sioux Falls, SD-MN

FIPS County Code	County Name	State	Proposed FY 2025 CBSA	Proposed FY 2025 CBSA Name
28009	BENTON	MS	32820	Memphis, TN-MS-AR
28123	SCOTT	MS	27140	Jackson, MS
30007	BROADWATER	MT	25740	Helena, MT
30031	GALLATIN	MT	14580	Bozeman, MT
30043	JEFFERSON	MT	25740	Helena, MT
30049	LEWIS AND CLARK	MT	25740	Helena, MT
30061	MINERAL	MT	33540	Missoula, MT
32019	LYON	NV	39900	Reno, NV
37125	MOORE	NC	38240	Pinehurst-Southern Pines, NC
38049	MCHENRY	ND	33500	Minot, ND
38075	RENVILLE	ND	33500	Minot, ND
38101	WARD	ND	33500	Minot, ND
39007	ASHTABULA	OH	17410	Cleveland, OH
39043	ERIE	OH	41780	Sandusky, OH
41013	CROOK	OR	13460	Bend, OR
41031	JEFFERSON	OR	13460	Bend, OR
42073	LAWRENCE	PA	38300	Pittsburgh, PA
45087	UNION	SC	43900	Spartanburg, SC
46033	CUSTER	SD	39660	Rapid City, SD
47081	HICKMAN	TN	34980	Nashville-Davidson--Murfreesboro--Franklin, TN
48007	ARANSAS	TX	18580	Corpus Christi, TX
48035	BOSQUE	TX	47380	Waco, TX
48079	COCHRAN	TX	31180	Lubbock, TX
48169	GARZA	TX	31180	Lubbock, TX
48219	HOCKLEY	TX	31180	Lubbock, TX
48323	MAVERICK	TX	20580	Eagle Pass, TX
48407	SAN JACINTO	TX	26420	Houston-Pasadena-The Woodlands, TX
51063	FLOYD	VA	13980	Blacksburg-Christiansburg-Radford, VA
51181	SURRY	VA	47260	Virginia Beach-Chesapeake-Norfolk, VA-NC
55123	VERNON	WI	29100	La Crosse-Onalaska, WI-MN

e. Urban Counties That Would Move to a Different Urban CBSA Under the Revised OMB Delineations

In addition to rural counties becoming urban and urban counties becoming rural, several urban counties would shift from one urban CBSA to a new or existing urban CBSA under our proposal to adopt the revised OMB delineations.

In other cases, applying the new OMB delineations would involve a change only in CBSA name or number, while the CBSA would continue to encompass the same constituent counties. For example, CBSA 35154 (New Brunswick-Lakewood, NJ) would experience both a change to its number and its name, and become CBSA 29484 (Lakewood-New Brunswick, NJ), while all three of its

constituent counties would remain the same. In other cases, only the name of the CBSA would be modified. Table 5 lists CBSAs that would change in name and/or CBSA number only, but the constituent counties would not change (except in instances where an urban county became rural, or a rural county became urban; as discussed in the previous section).

TABLE 5: Urban Areas With CBSA Name And/or Number Change

Current CBSA Code	Current CBSA Name	Proposed FY 2025 CBSA Code	Proposed FY 2025 CBSA Name
10380	Aguadilla-Isabela, PR	10380	Aguadilla, PR
10540	Albany-Lebanon, OR	10540	Albany, OR
12420	Austin-Round Rock-Georgetown, TX	12420	Austin-Round Rock-San Marcos, TX
12540	Bakersfield, CA	12540	Bakersfield-Delano, CA
13820	Birmingham-Hoover, AL	13820	Birmingham, AL
13980	Blacksburg-Christiansburg, VA	13980	Blacksburg-Christiansburg-Radford, VA
15260	Brunswick, GA	15260	Brunswick-St. Simons, GA
15680	California-Lexington Park, MD	30500	Lexington Park, MD
16540	Chambersburg-Waynesboro, PA	16540	Chambersburg, PA
16984	Chicago-Naperville-Evanston, IL	16984	Chicago-Naperville-Schaumburg, IL
17460	Cleveland-Elyria, OH	17410	Cleveland, OH
19430	Dayton-Kettering, OH	19430	Dayton-Kettering-Beavercreek, OH
19740	Denver-Aurora-Lakewood, CO	19740	Denver-Aurora-Centennial, CO
21060	Elizabethtown-Fort Knox, KY	21060	Elizabethtown, KY
21780	Evansville, IN-KY	21780	Evansville, IN
21820	Fairbanks, AK	21820	Fairbanks-College, AK
22660	Fort Collins, CO	22660	Fort Collins-Loveland, CO
23224	Frederick-Gaithersburg-Rockville, MD	23224	Frederick-Gaithersburg-Bethesda, MD
23844	Gary, IN	29414	Lake County-Porter County-Jasper County, IN
24340	Grand Rapids-Kentwood, MI	24340	Grand Rapids-Wyoming-Kentwood, MI
24860	Greenville-Anderson, SC	24860	Greenville-Anderson-Greer, SC
25940	Hilton Head Island-Bluffton, SC	25940	Hilton Head Island-Bluffton-Port Royal, SC
26380	Houma-Thibodaux, LA	26380	Houma-Bayou Cane-Thibodaux, LA
26420	Houston-The Woodlands-Sugar Land, TX	26420	Houston-Pasadena-The Woodlands, TX
26900	Indianapolis-Carmel-Anderson, IN	26900	Indianapolis-Carmel-Greenwood, IN
27900	Joplin, MO	27900	Joplin, MO-KS
27980	Kahului-Wailuku-Lahaina, HI	27980	Kahului-Wailuku, HI

Current CBSA Code	Current CBSA Name	Proposed FY 2025 CBSA Code	Proposed FY 2025 CBSA Name
29404	Lake County-Kenosha County, IL-WI	29404	Lake County, IL
29820	Las Vegas-Henderson-Paradise, NV	29820	Las Vegas-Henderson-North Las Vegas, NV
31020	Longview, WA	31020	Longview-Kelso, WA
34740	Muskegon, MI	34740	Muskegon-Norton Shores, MI
34820	Myrtle Beach-Conway-North Myrtle Beach, SC-NC	34820	Myrtle Beach-Conway-North Myrtle Beach, SC
35084	Newark, NJ-PA	35084	Newark, NJ
35154	New Brunswick-Lakewood, NJ	29484	Lakewood-New Brunswick, NJ
35840	North Port-Sarasota-Bradenton, FL	35840	North Port-Bradenton-Sarasota, FL
36084	Oakland-Berkeley-Livermore, CA	36084	Oakland-Fremont-Berkeley, CA
36260	Ogden-Clearfield, UT	36260	Ogden, UT
36540	Omaha-Council Bluffs, NE-IA	36540	Omaha, NE-IA
37460	Panama City, FL	37460	Panama City-Panama City Beach, FL
39100	Poughkeepsie-Newburgh-Middletown, NY	28880	Kiryas Joel-Poughkeepsie-Newburgh, NY
39340	Provo-Orem, UT	39340	Provo-Orem-Lehi, UT
39540	Racine, WI	39540	Racine-Mount Pleasant, WI
41540	Salisbury, MD-DE	41540	Salisbury, MD
41620	Salt Lake City, UT	41620	Salt Lake City-Murray, UT
42680	Sebastian-Vero Beach, FL	42680	Sebastian-Vero Beach-West Vero Corridor, FL
42700	Sebring-Avon Park, FL	42700	Sebring, FL
43620	Sioux Falls, SD	43620	Sioux Falls, SD-MN
44420	Staunton, VA	44420	Staunton-Stuarts Draft, VA
44700	Stockton, CA	44700	Stockton-Lodi, CA
45540	The Villages, FL	48680	Wildwood-The Villages, FL
47220	Vineland-Bridgeton, NJ	47220	Vineland, NJ
47260	Virginia Beach-Norfolk-Newport News, VA-NC	47260	Virginia Beach-Chesapeake-Norfolk, VA-NC
48140	Wausau-Weston, WI	48140	Wausau, WI
48300	Wenatchee, WA	48300	Wenatchee-East Wenatchee, WA
48424	West Palm Beach-Boca Raton-Boynton Beach, FL	48424	West Palm Beach-Boca Raton-Delray Beach, FL
49340	Worcester, MA-CT	49340	Worcester, MA
49660	Youngstown-Warren-Boardman, OH-PA	49660	Youngstown-Warren, OH

In some cases, all the urban counties from a FY 2024 CBSA would be moved and subsumed by another CBSA in FY

2025. Table 6 lists the CBSAs that, under our proposal to adopt the revised

OMB statistical area delineations, would be subsumed by another CBSA.

TABLE 6: Urban Areas Being Subsumed By Another CBSA

Current CBSA Code	Current CBSA Name	Proposed FY 2025 CBSA Code	Proposed FY 2025 CBSA Name
31460	Madera, CA	23420	Fresno, CA
36140	Ocean City, NJ	12100	Atlantic City-Hammonton, NJ
41900	San Germán, PR	32420	Mayagüez, PR

In other cases, if we adopt the new OMB delineations, some counties would shift between existing and new CBSAs, changing the constituent makeup of the CBSAs. In another type of change, some CBSAs have counties that would split off to become part of or to form entirely new labor market areas. For example, the District of Columbia, DC, Charles County, MD and Prince Georges County, MD would move from CBSA 47894

(Washington-Arlington-Alexandria, DC-VA-MD-WV) into CBSA 47764 (Washington, DC-Md). Calvert County, MD would move from CBSA 47894 (Washington-Arlington-Alexandria, DC-VA-MD-WV) into CBSA 30500 (Lexington Park, MD). The remaining counties that currently make up 47894 (Washington-Arlington-Alexandria, DC-VA-MD-WV) would move into CBSA 11694 (Arlington-Alexandria-Reston,

VA-WV). Finally, in some cases, a CBSA would lose counties to another existing CBSA if we adopt the new OMB delineations. For example, Grainger County, TN would move from CBSA 34100 (Morristown, TN) into CBSA 28940 (Knoxville, TN). Table 7 lists the 73 urban counties that would move from one urban CBSA to a new or modified urban CBSA if we adopt the revised OMB delineations.

TABLE 7: Counties That Would Change to a Different Urban CBSA

FIPS County Code	County Name	State	Current CBSA	Current CBSA Name	Proposed FY 2025 CBSA	Proposed FY 2025 CBSA Name
13013	BARROW	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13035	BUTTS	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13045	CARROLL	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13063	CLAYTON	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13077	COWETA	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13085	DAWSON	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13089	DE KALB	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13097	DOUGLAS	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13113	FAYETTE	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13117	FORSYTH	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13121	FULTON	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13135	GWINNETT	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13149	HEARD	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13151	HENRY	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13159	JASPER	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13199	MERIWETHER	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA

FIPS County Code	County Name	State	Current CBSA	Current CBSA Name	Proposed FY 2025 CBSA	Proposed FY 2025 CBSA Name
13211	MORGAN	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13217	NEWTON	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13227	PICKENS	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13231	PIKE	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13247	ROCKDALE	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13255	SPALDING	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13297	WALTON	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	12054	Atlanta-Sandy Springs-Roswell, GA
13015	BARTOW	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	31924	Marietta, GA
13057	CHEROKEE	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	31924	Marietta, GA
13067	COBB	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	31924	Marietta, GA
13143	HARALSON	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	31924	Marietta, GA
13223	PAULDING	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	31924	Marietta, GA
21163	MEADE	KY	21060	Elizabethtown-Fort Knox, KY	31140	Louisville/Jefferson County, KY-IN
17097	LAKE	IL	29404	Lake County-Kenosha County, IL-WI	29404	Lake County, IL
55059	KENOSHA	WI	29404	Lake County-Kenosha County, IL-WI	28450	Kenosha, WI
06039	MADERA	CA	31460	Madera, CA	23420	Fresno, CA
47057	GRAINGER	TN	34100	Morristown, TN	28940	Knoxville, TN
37019	BRUNSWICK	NC	34820	Myrtle Beach-Conway-North Myrtle Beach, SC-NC	48900	Wilmington, NC

FIPS County Code	County Name	State	Current CBSA	Current CBSA Name	Proposed FY 2025 CBSA	Proposed FY 2025 CBSA Name
22103	ST. TAMMANY	LA	35380	New Orleans-Metairie, LA	43640	Slidell-Mandeville-Covington, LA
34009	CAPE MAY	NJ	36140	Ocean City, NJ	12100	Atlantic City-Hammonton, NJ
72023	CABO ROJO	PR	41900	San Germán, PR	32420	Mayagüez, PR
72079	LAJAS	PR	41900	San Germán, PR	32420	Mayagüez, PR
72121	SABANA GRANDE	PR	41900	San Germán, PR	32420	Mayagüez, PR
72125	SAN GERMAN	PR	41900	San Germán, PR	32420	Mayagüez, PR
53061	SNOHOMISH	WA	42644	Seattle-Bellevue-Kent, WA	21794	Everett, WA
25015	HAMPSHIRE	MA	44140	Springfield, MA	11200	Amherst Town-Northampton, MA
12103	PINELLAS	FL	45300	Tampa-St. Petersburg-Clearwater, FL	41304	St. Petersburg-Clearwater-Largo, FL
12053	HERNANDO	FL	45300	Tampa-St. Petersburg-Clearwater, FL	45294	Tampa, FL
12057	HILLSBOROUGH	FL	45300	Tampa-St. Petersburg-Clearwater, FL	45294	Tampa, FL
12101	PASCO	FL	45300	Tampa-St. Petersburg-Clearwater, FL	45294	Tampa, FL
39123	OTTAWA	OH	45780	Toledo, OH	41780	Sandusky, OH
51013	ARLINGTON	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51043	CLARKE	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51047	CULPEPER	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51059	FAIRFAX	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51061	FAUQUIER	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51107	LOUDOUN	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51153	PRINCE WILLIAM	VA	47894	Washington-Arlington-	11694	Arlington-Alexandria-Reston, VA-WV

FIPS County Code	County Name	State	Current CBSA	Current CBSA Name	Proposed FY 2025 CBSA	Proposed FY 2025 CBSA Name
				Alexandria, DC-VA-MD-WV		
51157	RAPPAHANNOCK	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51177	SPOTSYLVANIA	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51179	STAFFORD	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51187	WARREN	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51510	ALEXANDRIA CITY	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51600	FAIRFAX CITY	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51610	FALLS CHURCH CITY	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51630	FREDERICKSBURG CITY	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51683	MANASSAS CITY	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
51685	MANASSAS PARK CITY	VA	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
54037	JEFFERSON	WV	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	11694	Arlington-Alexandria-Reston, VA-WV
11001	THE DISTRICT	DC	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	47764	Washington, DC-MD
24017	CHARLES	MD	47894	Washington-Arlington-	47764	Washington, DC-MD

FIPS County Code	County Name	State	Current CBSA	Current CBSA Name	Proposed FY 2025 CBSA	Proposed FY 2025 CBSA Name
				Alexandria, DC-VA-MD-WV		
24033	PRINCE GEORGES	MD	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	47764	Washington, DC-MD
24009	CALVERT	MD	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	30500	Lexington Park, MD
24037	ST. MARYS	MD	15680	California-Lexington Park, MD	30500	Lexington Park, MD
72059	GUAYANILLA	PR	49500	Yauco, PR	38660	Ponce, PR
72111	PENUELAS	PR	49500	Yauco, PR	38660	Ponce, PR
72153	YAUCO	PR	49500	Yauco, PR	38660	Ponce, PR

BILLING CODE 4120-01-C**f. Proposed Transition Period**

In the past we have provided for transition periods when adopting changes that have significant payment implications, particularly large negative impacts, in order to mitigate the potential impacts of proposed policies on hospices. For example, we have proposed and finalized budget-neutral transition policies to help mitigate negative impacts on hospices following the adoption of the new CBSA delineations based on the 2010 Decennial Census data in the FY 2016 hospice final rule (80 FR 47142). Specifically, we applied a blended wage index for one year (FY 2016) for all geographic areas that consisted of a 50/50 blend of the wage index values using OMB's old area delineations and the wage index values using OMB's new area delineations. That is, for each county, a blended wage index was calculated equal to 50 percent of the FY 2016 wage index using the old labor market area delineation and 50 percent of the FY 2016 wage index using the new labor market area delineations, which resulted in an average of the two values. Additionally, in the FY 2021 hospice final rule (85 FR 47079 through 47080), we proposed and finalized a transition policy to apply a 5-percent cap on any decrease in a geographic area's wage index value from the wage index value from the prior FY. This transition allowed the effects of our adoption of the revised CBSA delineations from OMB Bulletin 18-04 to be phased in over 2 years, where the

estimated reduction in a geographic area's wage index was capped at five percent in FY 2021 (that is, no cap was applied to the reduction in the wage index for the second year (FY 2022)). We explained that we believed a 5-percent cap on the overall decrease in a geographic area's wage index value would be appropriate for FY 2021, as it provided predictability in payment levels from FY 2020 to FY 2021 and additional transparency because it was administratively simpler than our prior one-year 50/50 blended wage index approach.

As discussed previously, in the FY 2023 hospice final rule, we adopted a permanent 5-percent cap on wage index decreases beginning in FY 2023 and each subsequent year (87 FR 45677). The policy applies a permanent 5-percent cap on any decrease to a geographic area's wage index from its wage index in the prior year, regardless of the circumstances causing the decline, so that a geographic area's wage index would not be less than 95 percent of its wage index calculated in the prior FY.

For FY 2025, we believe that the permanent 5-percent cap on wage index decreases would be sufficient to mitigate any potential negative impact for hospices serving beneficiaries in areas that are impacted by the proposal to adopt the revised OMB delineations and that no further transition is necessary. Previously, the 5-percent cap had been applied at the CBSA or statewide rural area level, meaning that all the counties that make up the CBSA

or rural area received the 5-percent cap. However, for FY 2025, to mitigate any potential negative impact caused by our proposed adoption of the revised delineations, we propose that in addition to the 5-percent cap being calculated for an entire CBSA or statewide rural area the cap would also be calculated at the county level, so that individual counties moving to a new delineation would not experience more than a 5 percent decrease in wage index from the previous fiscal year. Specifically, we are proposing for FY 2025, that the 5-percent cap would also be applied to counties that would move from a CBSA or statewide rural area with a higher wage index value into a new CBSA or rural area with a lower wage index value, so that the county's FY 2025 wage index would not be less than 95 percent of the county's FY 2024 wage index value under the old delineation despite moving into a new delineation with a lower wage index.

Due to the way that we propose to calculate the 5-percent cap for counties that experience an OMB designation change, some CBSAs and statewide rural areas could have more than one wage index value because of the potential for their constituent counties to have different wage index values as a result of application of the 5-percent cap. Specifically, some counties that change OMB designations would have a wage index value that is different than the wage index value assigned to the other constituent counties that make up the CBSA or statewide rural area that they are moving into because of the

application of the 5-percent cap. However, for hospice claims processing, each CBSA or statewide rural area can have only one wage index value assigned to that CBSA or statewide rural area.

Therefore, hospices that serve beneficiaries in a county that would receive the cap would need to use a number other than the CBSA or statewide rural area number to identify the county's appropriate wage index value for hospice claims in FY 2025. We are proposing that beginning in FY 2025, counties that have a different wage index value than the CBSA or rural area into which they are designated after the application of the 5-percent cap would use a wage index transition code. These special codes are five digits in length and begin with "50." The 50XXX wage index transition codes would be used only in specific counties; counties located in CBSAs and rural areas that do not correspond to a different transition wage index value will still use the CBSA number. For

example, FIPS county 13171 Lamar County, GA is currently part of CBSA 12060 Atlanta-Sandy Springs-Alpharetta. However, for FY 2025 we are proposing that Lamar County would be redesignated into the Rural Georgia Code 99911. Because the wage index value of rural Georgia is more than a 5-percent decrease from the wage index value that Lamar County previously received under CBSA 12060, the FY 2025 wage index for Lamar County would be capped at 95 percent of the FY 2024 wage index value for CBSA 12060. Additionally, because rural Georgia can only have one wage index value assigned to code 99911, in order for Lamar County to receive the capped wage index for FY 2025, transition code 50002 would be used instead of rural Georgia code 99911.

Additionally, we are proposing that the 5-percent cap would apply to a county that corresponds to a different wage index value than the wage index value in the CBSA or rural area in which they are designated due to a

delineation change until the county's new wage index is more than 95 percent of the wage index from the previous fiscal year. We are also proposing that in order to capture the correct wage index value, the county would continue to use the assigned 50XXX transition code until the county's wage index value calculated for the that fiscal year using the new OMB delineations is not less than 95 percent of the county's capped wage index from the previous fiscal year. Thus, in the example mentioned above, Lamar County would continue to use transition code 50002 until the wage index in its revised designation of Rural Georgia is equal to or more than 95 percent of its wage index value from the previous fiscal year. The counties that will require a transition code and the corresponding 50XXX codes are shown in Table 8 and will also be shown in the last column of the FY 2025 hospice wage index file.

BILLING CODE 4120-01-P

TABLE 8: Counties That Will Use a Wage Index Transition Code

FIPS Code	County Name	State	FY 2024 CBSA	FY 2024 CBSA Name	Proposed FY 2025 CBSA	Proposed FY 2025 CBSA Name	Proposed Transition Code
01129	WASHINGTON	AL	33660	Mobile, AL	99901	ALABAMA	50001
13171	LAMAR	GA	12060	Atlanta-Sandy Springs-Alpharetta, GA	99911	GEORGIA	50002
15005	KALAWAO	HI	99912	HAWAII	27980	Kahului-Wailuku, HI	50003
16077	POWER	ID	38540	Pocatello, ID	99913	IDAHO	50004
17183	VERMILION	IL	19180	Danville, IL	99914	ILLINOIS	50005
18133	PUTNAM	IN	26900	Indianapolis-Carmel-Anderson, IN	99915	INDIANA	50006
21101	HENDERSON	KY	21780	Evansville, IN-KY	99918	KENTUCKY	50007
24009	CALVERT	MD	47894	Washington-Arlington-Alexandria, DC-VA-MD-WV	30500	Lexington Park, MD	50008
24047	WORCESTER	MD	41540	Salisbury, MD-DE	99921	MARYLAND	50009
25011	FRANKLIN	MA	44140	Springfield, MA	99922	MASSACHUSETTS	50010
26155	SHIAWASSEE	MI	29620	Lansing-East Lansing, MI	99923	MICHIGAN	50011
27075	LAKE	MN	20260	Duluth, MN-WI	99924	MINNESOTA	50012
27133	ROCK	MN	99924	MINNESOTA	43620	Sioux Falls, SD-MN	50013
32019	LYON	NV	99929	NEVADA	39900	Reno, NV	50014
36123	YATES	NY	40380	Rochester, NY	99933	NEW YORK	50015
37077	GRANVILLE	NC	20500	Durham-Chapel Hill, NC	99934	NORTH CAROLINA	50016
37087	HAYWOOD	NC	11700	Asheville, NC	99934	NORTH CAROLINA	50017
39123	OTTAWA	OH	45780	Toledo, OH	41780	Sandusky, OH	50018
42103	PIKE	PA	35084	Newark, NJ-PA	99939	PENNSYLVANIA	50019
51113	MADISON	VA	47894	Washington-Arlington-	99949	VIRGINIA	50020

				Alexandria, DC-VA-MD-WV			
51175	SOUTHAMPTON	VA	47260	Virginia Beach-Norfolk-Newport News, VA-NC	99949	VIRGINIA	50021
51620	FRANKLIN CITY	VA	47260	Virginia Beach-Norfolk-Newport News, VA-NC	99949	VIRGINIA	50021
54057	MINERAL	WV	19060	Cumberland, MD-WV	99951	WEST VIRGINIA	50022
72001	ADJUNTAS	PR	38660	Ponce, PR	99940	PUERTO RICO	50023
72023	CABO ROJO	PR	41900	San Germán, PR	32420	Mayagüez, PR	50024
72055	GUANICA	PR	49500	Yauco, PR	99940	PUERTO RICO	50025
72079	LAJAS	PR	41900	San Germán, PR	32420	Mayagüez, PR	50024
72081	LARES	PR	10380	Aguadilla-Isabela, PR	99940	PUERTO RICO	50026
72083	LAS MARIAS	PR	32420	Mayagüez, PR	99940	PUERTO RICO	50027
72121	SABANA GRANDE	PR	41900	San Germán, PR	32420	Mayagüez, PR	50024
72125	SAN GERMAN	PR	41900	San Germán, PR	32420	Mayagüez, PR	50024
72141	UTUADO	PR	10380	Aguadilla-Isabela, PR	99940	PUERTO RICO	50026

BILLING CODE 4120-01-C

The proposed wage index applicable to FY 2025 provides a crosswalk between the FY 2025 wage index using the current OMB delineations and the FY 2025 wage index using the proposed revised OMB delineations that would be in effect in FY 2025 if these proposed changes are finalized. This file shows each State and county and its corresponding proposed wage index along with the previous CBSA number, the proposed CBSA number or alternate identification number, and the proposed CBSA name. The proposed hospice wage index file applicable for FY 2025 (October 1, 2024 through September 30, 2025) is available on the CMS website at: <https://www.cms.gov/medicare/payment/fee-for-service-providers/hospice/hospice-regulations-and-notice>.

3. Proposed FY 2025 Hospice Payment Update Percentage

Section 4441(a) of the Balanced Budget Act of 1997 (BBA) (Pub. L. 105-33) amended section 1814(i)(1)(C)(ii)(VI) of the Act to establish updates to hospice rates for FYs 1998 through 2002. Hospice rates were to be updated by a factor equal to the inpatient hospital market basket percentage increase set out under section

1886(b)(3)(B)(iii) of the Act, minus one percentage point. Payment rates for FYs since 2002 have been updated according to section 1814(i)(1)(C)(ii)(VII) of the Act, which states that the update to the payment rates for subsequent FYs must be the inpatient hospital market basket percentage increase for that FY. In the FY 2022 IPPS final rule, we finalized the rebased and revised IPPS market basket to reflect a 2018 base year. We refer readers to the FY 2022 IPPS final rule (86 FR 45194) for further information.

Section 3401(g) of the Affordable Care Act mandated that, starting with FY 2013 (and in subsequent FYs), the hospice payment update percentage would be annually reduced by changes in economy-wide productivity as specified in section 1886(b)(3)(B)(xi)(II) of the Act. The statute defines the productivity adjustment to be equal to the 10-year moving average of changes in annual economy-wide private nonfarm business multifactor productivity (MFP) as projected by the Secretary for the 10-year period ending with the applicable FY, year, cost reporting period, or other annual period (the “productivity adjustment”). The United States Department of Labor’s Bureau of Labor Statistics (BLS)

publishes the official measures of productivity for the United States economy. We note that previously the productivity measure referenced in section 1886(b)(3)(B)(xi)(II) of the Act was published by BLS as private nonfarm business multifactor productivity. Beginning with the November 18, 2021 release of productivity data, BLS replaced the term “multifactor productivity” with “total factor productivity” (TFP). BLS noted that this is a change in terminology only and would not affect the data or methodology. As a result of the BLS name change, the productivity measure referenced in section 1886(b)(3)(B)(xi)(II) of the Act is now published by BLS as “private nonfarm business total factor productivity.” However, as mentioned, the data and methods are unchanged. We refer readers to <http://www.bls.gov> for the BLS historical published TFP data. A complete description of IGI’s TFP projection methodology is available on the CMS website at <https://www.cms.gov/data-research/statistics-trends-and-reports/medicare-program-rates-statistics/market-basket-research-and-information>. In addition, in the FY 2022 IPPS final rule (86 FR 45214), we noted that beginning with FY 2022,

CMS changed the name of this adjustment to refer to it as the “productivity adjustment” rather than the “MFP adjustment”.

Consistent with our historical practice, we estimate the market basket percentage increase and the productivity adjustment based on IHS Global Inc.’s (IGI’s) forecast using the most recent available data. The proposed hospice payment update percentage for FY 2025 is based on the most recent estimate of the inpatient hospital market basket (based on IGI’s fourth quarter 2023 forecast with historical data through the third quarter of 2023). Due to the requirements at sections 1886(b)(3)(B)(xi)(II) and 1814(i)(1)(C)(v) of the Act, the proposed inpatient hospital market basket percentage increase for FY 2025 of 3.0 percent is required to be reduced by a productivity adjustment as mandated by section 3401(g) of the Affordable Care Act. The proposed productivity adjustment for FY 2025 is 0.4 percentage point (based on IGI’s fourth quarter 2023 forecast). Therefore, the proposed hospice payment update percentage for FY 2025 is 2.6 percent. We also propose that if more recent data become available after the publication of this proposed rule and before the publication of the final rule (for example, a more recent estimate of the inpatient hospital market basket percentage increase or productivity adjustment), we would use such data, if appropriate, to determine the hospice payment update percentage in the FY 2025 final rule.

We continue to believe it is appropriate to routinely update the hospice payment system so that it reflects the best available data about differences in patient resource use and costs among hospices as required by the statute. Therefore, we are proposing to update hospice payments using the methodology outlined and apply the 2018-based IPPS market basket percentage increase for FY 2025 of 3.0 percent, reduced by the statutorily required productivity adjustment of 0.4 percentage point along with the wage index budget neutrality adjustment to update the payment rates. For the FY 2025 hospice wage index, we are proposing to use the FY 2025 pre-floor, pre-reclassified IPPS hospital wage

index with the proposed revised OMB labor market delineations as its basis.

In the FY 2022 Hospice Wage Index final rule (86 FR 42532), we rebased and revised the labor shares for RHC, CHC, GIP, and IRC using Medicare cost report data for freestanding hospices (CMS Form 1984–14, OMB Control Number 0938–0758) from 2018. The current labor portion of the payment rates are: RHC, 66.0 percent; CHC, 75.2 percent; GIP, 63.5 percent; and IRC, 61.0 percent. The non-labor portion is equal to 100 percent minus the labor portion for each level of care. The non-labor portion of the payment rates are as follows: RHC, 34.0 percent; CHC, 24.8 percent; GIP, 36.5 percent; and IRC, 39.0 percent.

4. Proposed FY 2025 Hospice Payment Rates

There are four payment categories that are distinguished by the location and intensity of the hospice services provided. The base payments are adjusted for geographic differences in wages by multiplying the labor share, which varies by category, of each base rate by the applicable hospice wage index. A hospice is paid the RHC rate for each day the beneficiary is enrolled in hospice, unless the hospice provides CHC, IRC, or GIP. CHC is provided during a period of patient crisis to maintain the patient at home; IRC is short-term care to allow the usual caregiver to rest and be relieved from caregiving; and GIP care is intended to treat symptoms that cannot be managed in another setting.

As discussed in the FY 2016 Hospice Wage Index and Rate Update final rule (80 FR 47172), we implemented two different RHC payment rates, one RHC rate for the first 60 days and a second RHC rate for days 61 and beyond. In addition, in that final rule, we implemented a Service Intensity Add-On (SIA) payment for RHC when direct patient care is provided by a registered nurse (RN) or social worker during the last seven days of the beneficiary’s life. The SIA payment is equal to the CHC hourly rate multiplied by the hours of nursing or social work provided (up to four hours total) that occurred on the day of service if certain criteria are met. To maintain budget neutrality, as required under section 1814(i)(6)(D)(ii) of the Act, the new RHC rates were

adjusted by an SIA budget neutrality factor (SBNF). The SBNF is used to reduce the overall RHC rate in order to ensure that SIA payments are budget neutral. At the beginning of every FY, SIA utilization is compared to the prior year in order to calculate a budget neutrality adjustment. For FY 2025, the proposed SIA budget neutrality factor is 1.009 for RHC days 1–60 and 1.000 for RHC days 61+.

In the FY 2017 Hospice Wage Index and Rate Update final rule (81 FR 52156), we initiated a policy of applying a wage index standardization factor to hospice payments in order to eliminate the aggregate effect of annual variations in hospital wage data. For FY 2025 hospice rate setting, we are continuing our longstanding policy of using the most recent data available. Specifically, we are proposing to use FY 2023 claims data as of January 11, 2024 for the proposed FY 2025 payment rate updates. We note that the budget neutrality factors and payment rates will be updated with more complete FY 2023 claims data for the final rule. In order to calculate the wage index standardization factor, we simulate total payments using FY 2023 hospice utilization claims data with the FY 2024 wage index (pre-floor, pre-reclassified hospital wage index with the hospice floor, old OMB delineations, and the 5-percent cap on wage index decreases) and FY 2024 payment rates and compare it to our simulation of total payments using FY 2023 utilization claims data, the proposed FY 2025 hospice wage index (pre-floor, pre-reclassified hospital wage index with hospice floor, and the revised OMB delineations, with the 5-percent cap on wage index decreases) and FY 2024 payment rates. By dividing payments for each level of care (RHC days 1 through 60, RHC days 61+, CHC, IRC, and GIP) using the FY 2024 wage index and FY 2024 payment rates for each level of care by the FY 2025 wage index and FY 2024 payment rates, we obtain a wage index standardization factor for each level of care. The wage index standardization factors for each level of care are shown in Tables 1 and 2.

The proposed FY 2025 RHC rates are shown in Table 9. The FY 2025 payment rates for CHC, IRC, and GIP are shown in Table 10.

TABLE 9: Proposed FY 2025 Hospice RHC Payment Rates-

Code	Description	FY 2024 Payment Rates	SIA Budget Neutrality Factor	Wage Index Standardization Factor	FY 2025 Hospice Payment Update	Proposed FY 2025 Payment Rates
651	Routine Home Care (days 1-60)	\$218.33	1.0009	0.9983	1.026	\$223.83
651	Routine Home Care (days 61+)	\$172.35	1.0000	0.9975	1.026	\$176.39

TABLE 10: Proposed FY 2025 Hospice CHC, IRC, and GIP Payment Rates

Code	Description	FY 2024 Payment Rates	Wage Index Standardization Factor	FY 2025 Hospice Payment Update	Proposed FY 2025 Payment Rates
652	Continuous Home Care Full Rate = 24 hours of care.	\$1,565.46	1.0026	1.026	\$1,610.34 (\$67.10 per hour)
655	Inpatient Respite Care	\$507.71	0.9947	1.026	\$518.15
656	General Inpatient Care	\$1,145.31	0.9931	1.026	\$1,166.98

Sections 1814(i)(5)(A) through (C) of the Act require that hospices submit quality data on measures to be specified by the Secretary. In the FY 2012 Hospice Wage Index and Rate Update final rule (76 FR 47320 through 47324), we implemented a Hospice Quality Reporting Program (HQRP) as required by those sections. Hospices were required to begin collecting quality data in October 2012 and submit those quality data in 2013. Section 1814(i)(5)(A)(i) of the Act requires that beginning with FY 2014 through FY 2023, the Secretary shall reduce the market basket percentage increase by

two percentage points for any hospice that does not comply with the quality data submission requirements with respect to that FY. Section 1814(i)(5)(A)(i) of the Act was amended by section 407(b) of Division CC, Title IV of the Consolidated Appropriations Act (CAA), 2021 (Pub. L. 116-260) to change the payment reduction for failing to meet hospice quality reporting requirements from two to four percentage points. Depending on the amount of the annual update for a particular year, a reduction of 4 percentage points beginning in FY 2024 could result in the annual market basket

update being less than zero percent for a FY and may result in payment rates that are less than payment rates for the preceding FY. We applied this policy beginning with the FY 2024 Annual Payment Update (APU), which we based on CY 2022 quality data. Therefore, the proposed FY 2025 rates for hospices that do not submit the required quality data would be updated by -1.4 percent, which is the proposed FY 2025 hospice payment update percentage of 2.6 percent minus four percentage points. These rates are shown in Tables 11 and 12.

TABLE 11: Proposed FY 2025 Hospice RHC Payment Rates for Hospices That DO NOT Submit the Required Quality Data

Code	Description	FY 2024 Payment Rates	SIA Budget Neutrality Factor	Wage Index Standardization Factor	FY 2025 Hospice Payment Update of 2.6% minus 4 percentage points = - 1.4%	Proposed FY 2025 Payment Rates
651	Routine Home Care (days 1-60)	\$218.33	1.0009	0.9983	0.9860	\$215.10
651	Routine Home Care (days 61+)	\$172.35	1.0000	0.9975	0.9860	\$169.51

TABLE 12: Proposed FY 2025 Hospice CHC, IRC, and GIP Payment Rates for Hospices That DO NOT Submit the Required Quality Data

Code	Description	FY 2024 Payment Rates	Wage Index Standardization Factor	FY 2025 Hospice Payment Update of 2.6% minus 4 percentage points = - 1.4%	Proposed FY 2025 Payment Rates
652	Continuous Home Care Full Rate = 24 hours of care.	\$1,565.46	1.0026	0.9860	\$1,547.56 (64.48 per hour)
655	Inpatient Respite Care	\$507.71	0.9947	0.9860	\$497.95
656	General Inpatient Care	\$1,145.31	0.9931	0.9860	\$1,121.48

5. Proposed Hospice Cap Amount for FY 2025

As discussed in the FY 2016 Hospice Wage Index and Rate Update final rule (80 FR 47183), we implemented changes mandated by the IMPACT Act of 2014. Specifically, we stated that for accounting years that end after September 30, 2016 and before October 1, 2025, the hospice cap is updated by the hospice payment update percentage rather than using the CPI-U. Division CC, section 404 of the CAA, 2021 extended the accounting years impacted by the adjustment made to the hospice

cap calculation until 2030. In the FY 2022 Hospice Wage Index final rule (86 FR 42539), we finalized conforming regulations text changes at § 418.309 to reflect the provisions of the CAA, 2021. Division P, section 312 of the CAA, 2022 (Pub. L. 117-103) amended section 1814(i)(2)(B) of the Act and extended the provision that mandates the hospice cap be updated by the hospice payment update percentage (the inpatient hospital market basket percentage increase reduced by the productivity adjustment) rather than the CPI-U for accounting years that end after

September 30, 2016 and before October 1, 2031. Division FF, section 4162 of the CAA, 2023 (Pub. L. 118-328) amended section 1814(i)(2)(B) of the Act and extended the provision that currently mandates the hospice cap be updated by the hospice payment update percentage (the inpatient hospital market basket percentage increase reduced by the productivity adjustment) rather than the CPI-U for accounting years that end after September 30, 2016 and before October 1, 2032. Division G, Section 308 of the Consolidated Appropriations Act of 2024 (CAA, 2024) (Pub. L. 118-42)

extends this provision to October 1, 2033. Before the enactment of this provision, the hospice cap update was set to revert to the original methodology of updating the annual cap amount by the CPI-U beginning on October 1, 2032. Therefore, for accounting years that end after September 30, 2016 and before October 1, 2033, the hospice cap amount is updated by the hospice payment update percentage rather than the CPI-U. As a result of the changes mandated by the CAA, 2024, we propose conforming regulation text changes at § 418.309 to reflect the revisions at section 1814(i)(2)(B) of the Act.

The proposed hospice cap amount for the FY 2025 cap year is \$34,364.85, which is equal to the FY 2024 cap amount (\$33,494.01) updated by the proposed FY 2025 hospice payment update percentage of 2.6 percent. We also propose that if more recent data become available after the publication of this proposed rule and before the publication of the final rule (for example, a more recent estimate of the hospice payment update percentage), we would use such data, if appropriate, to determine the hospice cap amount in the FY 2025 final rule.

B. Proposed Clarifying Regulation Text Changes

1. Medical Director Condition of Participation

CMS has broad statutory authority to establish health and safety standards for most Medicare- and Medicaid-participating provider and supplier types. The Secretary gives CMS the authority to enact regulations that are in the interest of the health and safety of individuals who are furnished services in an institution, while other laws, as outlined below, give CMS the authority to prescribe regulations as may be necessary to carry out the administration of the program. Section 122 of the Tax Equity and Fiscal Responsibility Act of 1982 (TEFRA) (Pub. L. 97-248), added section 1861(dd) to the Act to provide coverage for hospice care to terminally ill Medicare beneficiaries who elect to receive care from a Medicare-participating hospice. The CoPs apply to the hospice as an entity, as well as to the services furnished to each individual patient under hospice care. In accordance with section 1861(dd) of the Act, the Secretary is responsible for ensuring that the CoPs are adequate to protect the health and safety of the individuals under hospice care.

Based on feedback from interested parties, including hospice providers,

national hospice associations, and accrediting organizations, we identified discrepancies between the Medical Director CoP at § 418.102 and the payment requirements for the “certification of the terminal illness” and the “admission to hospice care” at § 418.22 and § 418.25, respectively. Specifically, the industry questioned the language in the requirements as it relates to medical directors in the CoPs, physician designees in the CoPs, and physician members of the interdisciplinary group (IDG) in the payment requirements. Currently, the medical director provisions in the CoPs at §§ 418.102(b) and (c) require the medical director or physician designee to review the clinical information for each patient and provide written certification that it is anticipated that the patient’s life expectancy is 6 months or less if the illness runs its normal course. However, the statutory requirements in section 1814(a)(7)(A)(i)(II) and (ii) of the Act and the regulatory payment requirements at § 418.22 (*Certification of terminal illness*) provide that the medical director of the hospice or the physician member of the hospice interdisciplinary group can certify the patient’s terminal illness. Although the CoP provisions at §§ 418.102(b) and (c) include requirements for the initial certification and recertification of terminal illness, they do not include the physician member of the interdisciplinary group among the types of practitioners who can provide these certifications, even though these physicians are able to certify terminal illness under the payment regulation at § 418.22 (*Certification of terminal illness*).

This misalignment between the CoPs and the payment requirements has caused some confusion for hospice providers, accrediting bodies, and surveyors. As a result, we determined that conforming changes should be proposed to the medical director CoP for clarity and consistency. To align the medical director CoP and the hospice payment requirements, we propose to amend § 418.102(b) by adding the physician member of the hospice interdisciplinary group as defined in § 418.56(a)(1)(i), as an individual who may provide the initial certification of terminal illness. We also propose to amend the medical director CoP § 418.102(c) to include the medical director, or physician designee, as defined at § 418.3, if the medical director is not available, or physician member of the IDG among the specified physicians who may review the clinical

information as part of the recertification of the terminal illness.

We refer readers to section III.B.2 of this proposed rule for additional proposals regarding the payment requirements for the certification of the terminal illness and admission to hospice care under §§ 418.22 and 418.25, which are also intended to align the medical director CoP and payment regulations.

2. Certification of Terminal Illness and Admission to Hospice Care

The Medicare hospice benefit provides coverage for a comprehensive set of services described in section 1861(dd)(1) of the Act for individuals who are deemed “terminally ill” based on a medical prognosis that the individual’s life expectancy is 6 months or less, as described in section 1861(dd)(3)(A) of the Act.

As such, section 1814(a)(7)(A) of the Act requires the individual’s attending physician (if the patient designates an attending) and hospice medical director or physician member of the hospice interdisciplinary group (IDG) to certify in writing at the beginning in the first 90-day period of hospice care that the individual is “terminally ill” based on the physician’s or medical director’s clinical judgment regarding the normal course of the individual’s illness. In a subsequent 90- or 60-day period of hospice care, only the hospice medical director or the physician member of the IDG is required to recertify at the beginning of the period that the patient is terminally ill based on such clinical judgment.

The Conditions of Participation (CoP) at § 418.102 state that “when the medical director is not available, a physician designated by the hospice assumes the same responsibilities and obligations as the medical director.” The term “physician designee” was utilized in the 1983 hospice final rule (48 FR 56029) that implemented the Medicare hospice benefit when describing who can establish and review the hospice plan of care and was later defined and finalized in the 2008 hospice final rule (73 FR 32093) in response to comments requesting CMS clarify this individual’s role. Section 418.3 defines “physician designee” to mean a doctor of medicine or osteopathy designated by the hospice who assumes the same responsibilities and obligations as the medical director when the medical director is not available. Currently, the requirements at § 418.22(c), Sources of Certification, state that for the initial 90-day period, the hospice must obtain written certification statements from the

medical director of the hospice or the physician member of the IDG and the individual's attending physician if the individual has an attending physician. For subsequent periods, only the "medical director of the hospice or the physician member of the interdisciplinary group" must certify terminal illness. Similarly, the requirements at § 418.22(b), Content of Certification, only include the "medical director of the hospice" or the "physician member of the hospice interdisciplinary group" when referencing the clinical judgment on which the certification must be based. Additionally, § 418.25, Admission to Hospice Care, only refers to the recommendation of the hospice medical director (in consultation with the patient's attending physician (if any)) when determining admission to hospice and when reaching a decision to certify that the patient is terminally ill. In order to align §§ 418.22(b) and 418.25 with the CoPs at § 418.102, we propose to add "physician designee (as defined in § 418.3)" to clarify that when the medical director is not available, a physician designated by the hospice, who is assuming the same responsibilities and obligations as the medical director, may certify terminal illness and determine admission to hospice care. We are clarifying that this does not connote a change in policy; rather we believe aligning the language at §§ 418.22(b) and 418.25 with the CoPs at § 418.102 allows for greater clarity and consistency between key components of hospice regulations and policies.

3. Election of Hospice Care

A distinctive characteristic of the Medicare hospice benefit is that it requires a patient (or their representative) to intentionally choose hospice care by electing the benefit. As part of the election required by § 418.24, a beneficiary (or their representative) must file an "election statement" with the hospice, which must include an acknowledgement that they fully understand the palliative, rather than curative, nature of hospice care as it relates to the individual's terminal illness and related conditions, as well as other requirements as set out at § 418.24(b). Additionally, as set out at § 418.24(f), when electing the hospice benefit, an individual waives all rights to Medicare payment for any care for the terminal illness and related conditions except for services provided by the designated hospice, another hospice under arrangement with the designated hospice, and the individual's attending physician if that physician is not an

employee of the designated hospice or receiving compensation from the hospice for those services. Because of this waiver, this means that the designated hospice is the only provider to which Medicare payment can be made for services related to the terminal illness and related conditions for the patient; providers other than the designated hospice, a hospice under arrangement with the designated hospice, or the individual's attending physician cannot receive payment for services to a hospice beneficiary unless those services are unrelated to the terminal illness and related conditions when a patient is under a hospice election.

In the FY 2015 Hospice Wage Index and Payment Rate Update final rule (79 FR 50452, 50478), we finalized a requirement that a Notice of Election (NOE) must be filed with the hospice Medicare Administrative Contractor (MAC) within five calendar days after the effective date of hospice election. If the NOE is filed beyond this timeframe, hospice providers are liable for the services furnished during the days from the effective date of hospice election to the date of NOE filing (79 FR 50478). Also, because non-hospice providers may be unaware of a hospice election, late filing of the NOE leaves Medicare vulnerable to paying non-hospice claims related to the terminal illness and related conditions when these services are furnished by these non-hospice providers. Moreover, beneficiaries may potentially be liable for any associated cost-sharing they would not have incurred if these services were furnished by the hospice provider.

When discussing hospice election, stakeholders (such as Medicare contractors, medical reviewers, and hospices) often conflate the terms "election statement" and "NOE." Further, we have received recent inquiries requesting clarification on timeframe requirements for both the election statement and the NOE that indicate confusion between such documents. Upon review of this regulation, we believe the organization at § 418.24 does not make it clear that these are two separate and distinct documents intended for separate purposes under the benefit. We propose to reorganize the language in this section to clearly denote the differences between the election statement and the NOE. That is, we are proposing to title § 418.24(b) as "Election Statement" and would include the title "Notice of Election" at § 418.24(e). By clearly titling this section, the requirements for the election statement and the notice of election would be distinguished from

one another, mitigating any confusion between the two documents. These changes align with existing subregulatory guidance. This reorganization would not be a change in policy, rather it is intended to more clearly identify the requirements for the election statement and the NOE by reorganizing the structure of the regulations. We believe this reorganization is important to ensure that stakeholders fully understand that the election statement is required as acknowledgement of a beneficiary's understanding of the decision to elect hospice and filed with the hospice, whereas the NOE is required for claims processing purposes and filed with the hospice MAC within five calendar days after the effective date of the election statement.

We invite comments on the clarifying regulation text changes and reorganization as described in sections II.B. of this proposed rule.

Finally, the MACs have informed us of ongoing instances of hospices omitting certain elements of the hospice election statement. A complete election statement containing all required elements as set forth at § 418.24(b) is a condition for payment. Additionally, we emphasize the importance of each element in informing the beneficiary of their coverage when choosing to elect the Medicare hospice benefit. We continue to encourage hospice agencies to utilize the "Model Example of Hospice Election Statement" on the hospice web page at <https://www.cms.gov/medicare/payment/fee-for-service-providers/hospice> to limit potential claims denials.

C. Request for Information (RFI) on Payment Mechanism for High Intensity Palliative Care Services

We define hospice care as a set of comprehensive services described in section 1861(dd)(1) of the Act, identified and coordinated by an interdisciplinary group (IDG) to provide for the physical, psychosocial, spiritual, and emotional needs of a terminally ill patient and/or family members, as delineated in a specific patient plan of care (§ 418.3). Hospice care changes the focus of a patient's illness to comfort care (palliative care) for pain relief and symptom management under a curative type of care. Under the hospice benefit, palliative care is defined as patient and family centered care that optimizes quality of life by anticipating, preventing, and treating suffering (§ 418.3). Palliative care throughout the continuum of illness involves addressing physical, intellectual, emotional, social, and spiritual needs

and facilitating patient autonomy, access to information, and choice. CMS continually works to ensure access to quality hospice care for all eligible Medicare beneficiaries by establishing, refining, readapting, and reinforcing policies to improve the value of care at the end of life for these beneficiaries. That is, we seek to strengthen the notion that in order to provide the highest level of care for hospice beneficiaries, we must provide ongoing focus to those services that enforce CMS' definitions of hospice and palliative care and eliminate any barriers to accessing hospice care.

Adequate care under the hospice benefit has consistently been associated with symptom reduction, less intensive care, decreased hospitalizations, improved outcomes from caregivers, lower overall costs, and higher alignment with patient preferences and family satisfaction.⁴ Although hospice use has grown considerably since the inception of the Medicare hospice benefit in 1983, there are still barriers that terminally ill and hospice benefit eligible beneficiaries may face when accessing hospice care. Specifically, the national trends⁵ that examine hospice enrollment and service utilization for those beneficiary populations with complex palliative needs and potentially high-cost medical care needs reveal that there may be an underuse of the hospice benefit, despite the demonstrated potential to both improve quality of care and lower costs.⁶

There is a subset of hospice eligible beneficiaries that would likely benefit from receiving palliative, rather than curative, chemotherapy, radiation, blood transfusions, and dialysis. Anecdotally, we have heard from beneficiaries and families their understanding that upon election of the hospice benefit, certain therapies such as dialysis, chemotherapy, radiation, and blood transfusions are not available to them, even if such therapies would

provide palliation for their symptoms. Generally, these patients report that they have been told by hospices that Medicare does not allow for the provision of these types of treatments upon hospice election. While these types of treatments are not intended to cure the patient's terminal illness, some practitioners, with input from the hospice IDG, may determine that, for some patients, these adjuvant treatment modalities would be beneficial for symptom control. In such instances, these palliative treatments would be covered under the hospice benefit because they are not intended to be curative. In the FY 2024 Hospice Final Rule (88 FR 51168), we noted in response to our RFI on hospice utilization; non-hospice spending; ownership transparency; and hospice election decision-making, that commenters stated providing complex palliative treatments and higher intensity levels of hospice care may pose financial risks to hospices when enrolling such patients. Commenters stated that the current bundled per diem payment is not reflective of the increased expenses associated with higher-cost and certain patient subgroups. As we continue to focus on improved access and value within the hospice benefit, we are soliciting public comment on the following questions:

- What could eliminate the financial risk commenters previously noted when providing complex palliative treatments and higher intensity levels of hospice care?
- What specific financial risks or costs are of particular concern to hospices that would prevent the provision of higher-cost palliative treatments when appropriate for some beneficiaries? Are there individual cost barriers which may prevent a hospice from providing higher-cost palliative care services? For example, is there a cost barrier related to obtaining the appropriate equipment (for example, dialysis machine)? Or is there a cost barrier related to the treatment itself (for example, obtaining the necessary drugs or access to specialized staff)?

- Should there be any parameters around when palliative treatments should qualify for a different type of payment? For example, we are interested in understanding from hospices who do provide these types of palliative treatments whether the patient is generally in a higher level of care (CHC, GIP) when the decision is made to furnish a higher-cost palliative treatment? Should an additional payment only be applicable when the patient is in RHC?

- Under the hospice benefit, palliative care is defined as patient and family centered care that optimizes quality of life by anticipating, preventing, and treating suffering (§ 418.3). In addition to this definition of palliative care, should CMS consider defining *palliative services*, specifically regarding high-cost treatments? Note, CMS is not seeking a change to the definition of *palliative care* but rather should CMS consider defining *palliative services* with regard to high-cost treatments?

- Should there be documentation that all other palliative measures have been exhausted prior to billing for a payment for a higher-cost treatment? If so, would that continue to be a barrier for hospices?

- Should there be separate payments for different types of higher-cost palliative treatments or one standard payment for any higher-cost treatment that would exceed the per-diem rate?

D. Proposals to the Hospice Quality Reporting Program (HQRP)

1. Background and Statutory Authority

The Hospice Quality Reporting Program (HQRP) specifies reporting requirements for the Hospice Item Set (HIS), administrative data, and Consumer Assessment of Healthcare Providers and Systems (CAHPS®) Hospice Survey. Section 1814(i)(5) of the Act requires the Secretary to establish and maintain a quality reporting program for hospices, and requires, beginning with FY 2014, that the Secretary reduce the market basket update by 2 percentage points. Section 1814(i)(5)(A)(i) of the Act was amended by section 407(b) of Division CC, Title IV of the CAA, 2021 to change the payment reduction for failing to meet hospice quality reporting requirements from 2 to 4 percentage points beginning in FY 2024 for any hospice that does not comply with the quality data submission requirements for that FY. In the FY 2024 Hospice final rule, we codified the application of the 4-percentage point payment reduction for failing to meet hospice quality reporting requirements and set completeness thresholds at § 418.312(j).

Depending on the amount of the annual update for a particular year, a reduction of 4 percentage points beginning in FY 2024 could result in the annual market basket update being less than zero percent for a FY and may result in payment rates that are less than payment rates for the preceding FY. Any reduction based on failure to comply with the reporting requirements, as required by section 1814(i)(5)(B) of the

⁴ Obermeyer Z, Makar M, Abujaber S, Dominici F, Block S, Cutler DM. Association Between the Medicare Hospice Benefit and Health Care Utilization and Costs for Patients With Poor-Prognosis Cancer. *JAMA*. 2014;312(18):1888–1896. doi:10.1001/jama.2014.14950.

⁵ Wachterman MW, Hailpern SM, Keating NL, Kurella Tamura M, O'Hare AM. Association Between Hospice Length of Stay, Health Care Utilization, and Medicare Costs at the End of Life Among Patients Who Received Maintenance Hemodialysis. *JAMA Intern Med*. 2018 Jun 1;178(6):792–799. doi: 10.1001/jamainternmed.2018.0256. PMID: 29710217; PMCID: PMC5988968.

⁶ Meier DE. Increased access to palliative care and hospice services: opportunities to improve value in health care. *Milbank Q*. 2011 Sep;89(3):343–80. doi: 10.1111/j.1468-0009.2011.00632.x. PMID: 21933272; PMCID: PMC3214714.

Act, would apply only for the specified year. Typically, about 18 percent of Medicare-certified hospices are found non-compliant with the HQRP reporting requirements annually and are subject to the APU payment reduction for a given FY.

In the FY 2014 Hospice Wage Index and Payment Rate Update final rule (78 FR 48234, 48257 through 48262), and in compliance with section 1814(i)(5)(C) of the Act, we finalized a new standardized patient-level data collection vehicle called the Hospice Item Set (HIS). We also finalized the specific collection of data items that support eight consensus-based entity (CBE)-endorsed measures for hospice.

In the FY 2015 Hospice Wage Index and Payment Rate Update final rule (79 FR 50452), we finalized national implementation of the CAHPS® Hospice Survey, a component of the CMS HQRP which is used to collect data on the experiences of hospice patients and the primary caregivers listed in their hospice records. Readers who want more information about the development of the survey, originally called the Hospice Experience of Care Survey, may refer to the FY 2014 and FY 2015 Hospice Wage Index and Payment Update final rules (78 FR 48261 and 79 FR 50452, respectively). National implementation commenced January 1, 2015. We adopted eight CAHPS® survey-based measures for the CY 2018 data collection period and for subsequent years. These eight measures are publicly reported on the Care Compare website.

In the FY 2016 Hospice Wage Index and Rate Update final rule (80 FR 47142, 47186 through 47188), we finalized the policy for retention of HQRP measures adopted for previous payment determinations and seven factors for removal. In that same final rule, we discussed how we would provide public notice through rulemaking of measures under consideration for removal, suspension, or replacement. We also stated that if we had reason to believe continued collection of a measure raised potential safety concerns, we would take immediate action to remove the measure from the HQRP and not wait for the annual rulemaking cycle. The measures would be promptly removed and we would immediately notify hospices and the public of such a decision through

the usual HQRP communication channels, including but not limited to listening sessions, email notifications, Open Door Forums, and Web postings. In such instances, the removal of a measure will be formally announced in the next annual rulemaking cycle.

On August 31, 2020, we added correcting language to the FY 2016 Hospice Wage Index and Payment Rate Update and Hospice Quality Reporting Requirements; Correcting Amendment (85 FR 53679) hereafter referred to as the FY 2021 HQRP Correcting Amendment. In this final rule, we made correcting amendments to 42 CFR 418.312 to correct technical errors identified in the FY 2016 Hospice Wage Index and Payment Rate Update final rule. Specifically, the FY 2021 HQRP Correcting Amendment (85 FR 53679) adds paragraph (i) to § 418.312 to reflect our exemptions and extensions requirements, which were referenced in the preamble but inadvertently omitted from the regulations text. Thus, these exemptions or extensions can occur when a hospice encounters certain extraordinary circumstances.

In the FY 2017 Hospice Wage Index and Payment Rate Update final rule, we finalized the “Hospice Visits When Death” is Imminent measure pair (HVWDII, Measure 1 and Measure 2), effective April 1, 2017. We refer the public to the FY 2017 Hospice Wage Index and Payment Rate Update final rule (81 FR 52144, 52163 through 52169) for a detailed discussion.

As stated in the FY 2019 Hospice Wage Index and Rate Update final rule (83 FR 38622, 38635 through 38648), we launched the Meaningful Measures initiative (which identifies high priority areas for quality measurement and improvement) to improve outcomes for patients, their families, and providers while also reducing burden on clinicians and providers. The Meaningful Measures initiative is not intended to replace any existing CMS quality reporting programs, but will help such programs identify and select individual measures. The Meaningful Measure Initiative areas are intended to increase measure alignment across our quality programs and other public and private initiatives. Additionally, it will point to high priority areas where there may be gaps in available quality measures while helping to guide our efforts to develop and implement

quality measures to fill those gaps. More information about the Meaningful Measures Initiative can be found at: <https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/QualityInitiativesGenInfo/MMF/General-info-Sub-Page.html>.

In the FY 2022 Hospice Wage Index and Payment Rate Update final rule (86 FR 42552), we finalized two new measures using claims data: (1) Hospice Visits in the Last Days of Life (HVLDDL); and (2) Hospice Care Index (HCI). We also removed the Hospice Visits when Death is Imminent (HVWDII) measure, as it was replaced by HVLDDL. We also finalized a policy that claims-based measures would use 8 quarters of data to publicly report on more hospices.

In addition, we removed the seven Hospice Item Set (HIS) Process Measures from the program as individual measures, and ceased their public reporting because, in our view, the HIS Comprehensive Assessment Measure is sufficient for measuring care at admission without the seven individual process measures. In the FY 2022 Hospice Wage Index and Rate Update final rule (86 FR 42553), we finalized § 418.312(b)(2), which requires hospices to provide administrative data, including claims-based measures, as part of the HQRP requirements for § 418.306(b). In that same final rule, we provided CAHPS Hospice Survey updates.

As finalized in the FY 2022 Hospice Wage Index and Payment Rate Update final rule (86 FR 42552), public data reflecting hospices' reporting of the two new claims-based quality measures (QMs), the “Hospice Visits in Last Days of Life” (HVLDDL) and the “Hospice Care Index” (HCI) measures, are available on the Care Compare/Provider Data Catalogue (PDC) web pages as of the August 2022 refresh. In the FY 2023 and FY 2024 Hospice Wage Index final rules, we did not propose any new quality measures. However, we provided updates on already-adopted measures. Table 13 shows the current quality measures in effect for the FY 2025 HQRP, which were finalized in the FY 2022 Hospice Wage Index and Payment Rate Update final rule and have been carried over in each subsequent year.

BILLING CODE 4120-01-P

TABLE: 13 Quality Measures in Effect for the Hospice Quality Reporting Program

Hospice Quality Reporting Program	
Hospice Item Set	
Hospice and Palliative Care Composite Process Measure—HIS-Comprehensive Assessment Measure at Admission includes:	
1.	Patients Treated with an Opioid who are Given a Bowel Regimen
2.	Pain Screening
3.	Pain Assessment
4.	Dyspnea Treatment
5.	Dyspnea Screening
6.	Treatment Preferences
7.	Beliefs/Values Addressed (if desired by the patient)
Administrative Data, including Claims-based Measures	
Hospice Visits in Last Days of Life (HVLDL)	
Hospice Care Index (HCI)	
1.	Continuous Home Care (CHC) or General Inpatient (GIP) Provided
2.	Gaps in Skilled Nursing Visits
3.	Early Live Discharges
4.	Late Live Discharges
5.	Burdensome Transitions (Type 1)—Live Discharges from Hospice Followed by Hospitalization and Subsequent Hospice Readmission
6.	Burdensome Transitions (Type 2)—Live Discharges from Hospice Followed by Hospitalization with the Patient Dying in the Hospital
7.	Per-beneficiary Medicare Spending
8.	Skilled Nursing Care Minutes per Routine Home Care (RHC) Day
9.	Skilled Nursing Minutes on Weekends
10.	Visits Near Death
CAHPS Hospice Survey	
CAHPS Hospice Survey	
1.	Communication with Family
2.	Getting timely help
3.	Treating patient with respect
4.	Emotional and spiritual support
5.	Help for pain and symptoms
6.	Training family to care for the patient
7.	Rating of this hospice
8.	Willing to recommend this hospice

BILLING CODE 4120-01-C**2. Proposal To Implement Two Process Quality Measures Based on Proposed HOPE Data Collection**

Section 1814(i)(5) of the Act requires the Secretary to establish and maintain a quality reporting program for hospices, develop and implement quality measures, and publicly report quality measures. In this proposed rule, we propose adding two process measures no sooner than CY 2027 to the HQRP calculated from data collected from HOPE: *Timely Reassessment of Pain Impact* and *Timely Reassessment*

of Non-Pain Symptom Impact. We propose to use the data collected from HOPE (see section III. D on the proposal to implement HOPE and associated PRA), which a nurse would assess at multiple time points during a hospice stay to collect data related to patients' symptoms during those assessments. We propose these two measures would determine whether a follow-up visit occurs within 48 hours of an initial assessment of moderate or severe symptom impact.

Symptom alleviation is an important aspect of hospice care, including both pain management and non-pain

symptom management. CMS has heard this feedback consistently from both clinicians and caregivers, including the Technical Expert Panel (TEP) which CMS convened from 2019 through 2023. At present, HQRP only has a component of a measure indicating whether the pain symptom was assessed, as a part of the comprehensive assessment at admission measure. This measure alone does not adequately measure whether hospices are alleviating hospice patients' symptoms throughout their hospice stay.

CMS considers symptom management an important domain to address further.

Therefore, we propose these new concepts on timely reassessment of symptoms with the support and input of hospice experts. For cases where a patient is assessed as having high (that is, more severe) symptom impact, practitioners suggest that good care processes include trying to follow-up with the patient and having in-person visits/reassessment within 48 hours to ensure treatment has helped alleviate and/or manage those symptoms. Therefore, we are proposing two process measures derived from HOPE data—*Timely Reassessment of Pain Impact* and *Timely Reassessment of Non-Pain Symptom Impact*—would capture these care processes.

Our paramount concern is the successful development of an HQRP that promotes the delivery of high-quality healthcare services. We seek to adopt measures for the HQRP that promote efficient and safer care. Our measure selection activities for the HQRP take into consideration input we receive from the CBE, as part of a pre-rulemaking process that we have established and are required to follow under section 1890A of the Act. The CBE convenes interested parties from multiple groups to provide CMS with recommendations on the Measures Under Consideration (MUC) list. This input informs how CMS selects certain categories of quality and efficiency measures as required by section 1890A(a)(3) of the Act. By February 1st of each year, the CBE must provide that input to CMS. For more details about the pre-rulemaking process, please visit the Partnership for Quality Measurement website at <https://p4qm.org/PRMR>.

We also take into account national priorities, such as those established by the Partnership for Quality Measurement, the HHS Strategic Plan, and the National Strategy for Quality Improvement in Healthcare located at <https://www.cms.gov/ccio/resources/forms-reports-and-other-resources/quality03212011a>. To the extent possible, we have sought to adopt measures that have been endorsed by the national CBE, recommended by multiple organizations of interested parties, and developed with the input of providers, payers, and other relevant stakeholders.

a. Measure Importance

The FY 2019 Hospice Wage Index final rule (83 FR 38622) introduced the Meaningful Measure Initiative to hospice providers to identify high priority areas for quality measurement and improvement. The Meaningful Measure Initiative areas are intended to

increase measure alignment across programs and other public and private initiatives. Additionally, the initiative points to high priority areas where there may be informational gaps in available quality measures. The initiative helps guide our efforts to develop and implement quality measures to fill those gaps and develop those concepts towards quality measures that meet the standards for public reporting. The goal of HQRP quality measure development is to identify measures from a variety of data sources that provide a window into hospice care services throughout the dying process, fit well with the hospice business model, and meet the objectives of the Meaningful Measures initiative.

To that end, the proposed *Timely Reassessment of Pain Impact* and *Timely Reassessment of Non-Pain Symptom Impact* measures will add value to HQRP by filling an identified informational gap in the current measure set. Specifically, the proposed *Timely Reassessment of Pain Impact* process measure will determine how many patients assessed with moderate or severe pain impact were reassessed by the hospice within two calendar days, and the proposed *Timely Reassessment of Non-Pain Symptom Impact* process measure will determine how many patients assessed with moderate or severe non-pain impact were reassessed by the hospice within two calendar days. Compared to the single existing HQRP measure that includes pain symptom assessment, the two proposed HOPE-based process measures will better reflect hospices' efforts to alleviate patients' symptoms on an ongoing basis.

b. Proposed Specifications of the Measures

We proposed that both the process measures based on HOPE data will be calculated using assessments collected at admission or the HOPE Update Visit (HUV) timepoints. Pain symptom severity and impact will be determined based on hospice patients' responses to the pain symptom impact data elements within HOPE. Non-pain symptom severity and impact will be determined based on patients' responses to the HOPE data elements related to shortness of breath, anxiety, nausea, vomiting, diarrhea, constipation, and agitation. Additional information regarding these data items and time points can be found in the draft HOPE Guidance Manual of the HOPE web page at <https://www.cms.gov/medicare/quality/hospice/hope> and the PRA package that accompanies this proposed rule can be accessed at <https://www.cms.gov/medicare/regulations-guidance/>

legislation/paperwork-reduction-act-1995/pa-listing. We propose that only in-person visits would count for the collection of data for these proposed measures—that is, telehealth calls would not count for a reassessment. We seek comment on whether only in-person visits are appropriate for collection of data for these proposed measures or if other types of visits, such as telehealth, should be included. We propose that a follow-up visit cannot be the same visit as the initial assessment, but it can occur later in the same day (as a separate visit).

For both the proposed *Timely Reassessment of Pain Impact* and proposed *Timely Reassessment of Non-Pain Symptom Impact* measures, we propose beneficiaries will be included in the denominator if they have a moderate or severe level of pain or non-pain symptom impact, respectively, at their initial assessment. However, we proposed that certain exclusions will apply to these denominators, such as beneficiaries who die or are discharged alive before the two-day window, if the patient/caregiver refused the reassessment visit, the hospice was unable to contact the patient/caregiver to perform the reassessment, the patient traveled outside the service area, or the patient was in the ER/hospital during the two-day follow-up window. In these situations, we propose that a hospice would be unable to conduct a reassessment due to circumstances beyond their control, and therefore these situations will not be included in the measure denominator.

We propose the numerators for these measures will reflect beneficiaries who did receive a timely symptom reassessment. These will include beneficiaries who receive a separate HOPE reassessment within two calendar days of the initial assessment (for example, if a pain has moderate or severe symptoms assessed on Sunday, the hospice would be expected to complete the reassessment on or before Tuesday).

c. Measure Reportability, Variability, and Validity

As part of developing these quality measures, CMS and their measure development contractor conducted simulations of measure reportability rates and measure variability. We used the results of the HOPE Beta Test to estimate HOPE data availability for a national population of hospice patients. Detailed information regarding reportability and variability testing is provided in the HOPE Beta Testing Report, available on the HOPE web page at <https://www.cms.gov/medicare/>

quality/hospice/hope. Additionally, CMS assessed each proposed quality measure face validity with input from TEP members convened in March 2023. Further information about our validity analysis is provided in the 2022–2023 HQRP TEP Report, available in the Downloads section of the HQRP Provider and Stakeholder Engagement page. Our reportability and variability analyses did not present concerns for the proposed HOPE-based process measures, and our validity analysis indicated that the proposed measures have high face validity.

d. Future Plans for Testing HOPE-Based Quality Measures

Testing of the two proposed process quality measures has thus far relied on data from the HOPE beta (field) test. We propose future measure testing to be conducted using a full sample of hospices collected after HOPE has been implemented nationally, to support further development of quality measures.

e. Public Engagement and Support

CMS engaged the public in multiple stages of HOPE-based measure development. To support measure development, CMS convened multiple technical expert panel (TEP) meetings which served as information gathering activities, consistent with the Meaningful Measure Initiative. The TEP consisted of experts in hospice and clinical quality measurement, and it has contributed to development of the HOPE tool and measure concepts since 2019. Based on early TEP input about measure prioritization, measure concept development focused on pain and non-pain symptoms. TEP members noted the importance of measuring the quality of pain and symptom management, as this is a key role of hospice. Through 2020 and 2021, the TEP provided further feedback on pain and non-pain symptom measure specifications. In Spring 2023, CMS convened the TEP a final time to review the final measure specifications, HOPE Beta test results, and rate face validity of the measure score. The TEP gave strong support for the proposed measure specifications, rated high face validity for these two process measures, and noted the importance of measuring the quality of pain management in hospice care. More information about the TEP meetings and recommendations can be found in the HQRP TEP Reports for 2019–2023, available on the Provider and Stakeholder Engagement web page. CMS also sought hospice provider input during the HOPE Beta Test to further inform the development of these HOPE-

based process measures. During beta testing, registered nurses (RNs) reported that the two-day window of HOPE symptom reassessment aligned with their usual practices. In this proposed rule, we solicit public comments on these two process measures.

f. Update on Future Quality Measure (QM) Development

As stated in the FY 2022 Hospice Wage Index final rule (86 FR 42528), we continue to consider developing hybrid quality measures that could be calculated from multiple data sources, such as claims, HOPE data, or other data sources (for example, CAHPS Hospice Survey). To support new measure development, our contractor convened technical expert panel (TEP) meetings in 2022 and 2023. The TEP agreed that CMS should consider applying several risk adjustment factors, such as age and diagnosis, to ensure comparable, representative comparisons between hospices. The TEP also suggested using length of hospice stay but not functional status as risk adjustment factor for hospice performance.

To support new HOPE-based measure development, our contractor convened technical expert panel (TEP) meetings between 2020 and 2023. The TEP recommended specifications for the two HOPE-based quality measures proposed in this Rule—*Timely Reassessment of Pain Impact* and *Timely Reassessment of Non-Pain Symptom Impact*. CMS also sought TEP input on several measurement concepts proposed for future quality measure development. Of these measurement concepts, the TEP supported CMS further developing the *Education for Medication Management* and *Wound Management Addressed in Plan of Care* process concepts. More information about the TEP recommendations can be found in the 2023 HQRP TEP Report, available on the Provider and Stakeholder Engagement web page. CMS will take the TEP's recommendations under consideration as we continue to develop HOPE-based quality measures.

Additional information about CMS's HOPE-based measure development efforts is available in the 2022–2023 HQRP TEP Summary Report (<https://www.cms.gov/files/document/2023-hqrp-tep-summary-report.pdf>) and the 2023 Information Gathering Report, available on the HQRP Provider and Stakeholder Engagement web page, or at <https://www.cms.gov/files/document/hospicequalityreportingprograminformationgatheringreport2023508.pdf>. For further details about the ongoing development of these measures, please visit the Partnership for Quality

Measurement website: <https://p4qm.org/>.

3. Proposal To Implement the Hospice Outcomes & Patient Evaluation (HOPE) Assessment Instrument

Section 1814(i)(5)(C) of the Act requires that each hospice submit data to the Secretary on quality measures specified by the Secretary. The data must be submitted in a form, manner, and at a time specified by the Secretary.

CMS has developed a new standardized patient level data collection tool, the Hospice Outcomes & Patient Evaluation or HOPE. In past rules, we have described this as a new collection tool, however we believe it is better characterized as a modification of, and functional replacement for, the existing HIS structure.

We propose to begin collecting the HOPE standardized patient level data collection tool on or after October 1, 2025, for proposed quality measures discussed in section 2. We propose that the HOPE assessment instrument would replace the HIS upon implementation, as discussed in section III. D6(b). In the FY 2020 Hospice Wage Index and Payment Rate Update and Hospice Quality Reporting Requirements final rule (84 FR 38484), we finalized the instrument name and discussed the primary objectives for HOPE. Specifically, HOPE would provide data for the HQRP quality measures and its requirements through standardized data collection; and provide additional clinical data that could inform future payment refinements. All data collected by the instrument are expected to be used for quality measures, as authorized under section 1814(i)(5)(C) of the Act, and only for quality measures under section 1814(i)(5)(D), of the Act, which will include the measures *Timely Reassessment of Pain Impact* and *Timely Reassessment of Non-Pain Symptom Impact* measures proposed in this Rule.

HOPE would be a component of implementing high-quality and safe hospice care for patients, Medicare beneficiaries and non-beneficiaries alike. HOPE would also contribute to the patient's plan of care through providing patient data throughout the hospice stay. We propose to collect data from multiple time points across the hospice stay, that would inform hospice providers potentially resulting in improved practice and care quality. Additional information about the draft HOPE tool and the data elements included therein are available at <https://www.cms.gov/medicare/quality/hospice/hope> discussed in the

Paperwork Reduction Act submission for this collection (CMS–10390).

We stated in the FY 2022 Hospice Wage Index and Payment Update final rule (86 FR 42528) that while the standardized patient assessment data elements for certain post-acute care providers required under the IMPACT Act of 2014 are not applicable to hospices, it would be reasonable to include some of those standardized elements that could appropriately and feasibly apply to hospice to the extent permitted by our statutory authority. Many patients move through other providers within the healthcare system to hospice. Therefore, considering tracking key demographic and social risk factor items that apply to hospice could support our goals for continuity of care, overall patient care and well-being, development of infrastructure for the interoperability of electronic health information, and health equity which is also discussed in this proposed rule. CMS will propose any additions of standardized elements in future rulemaking.

In the FY 2023 Hospice Final Rule (87 FR 45669), we outlined the testing phases HOPE has undergone, including cognitive, pilot, alpha testing, and national beta field testing. National beta testing, completed at the end of October 2022, allowed us to obtain input from participating hospice teams about the assessment instrument and field testing to refine and support the final draft items and time points for HOPE. It also allowed us to estimate the time to complete the HOPE elements and establish the interrater reliability of each item. For additional details and results from HOPE testing, see the HOPE Testing Report, available in the Downloads section of the HOPE page of the HQRP website.

We propose to adopt and implement HOPE as a standardized patient element set to replace the current Hospice Item Set (HIS). HOPE v1.0 would contain demographic, record processing, and patient-level standardized data elements that would be collected by all Medicare-certified hospices for all patients over the age of 18, regardless of payer source, to support HQRP quality measures. We propose new HOPE data elements that are collected in real-time to assess patients based on the hospice's interactions with the patient and family/caregiver, accommodate patients with varying clinical needs, and provide additional information to contribute to the patient's care plan throughout the hospice stay (not just at admission and discharge). These data elements represent domains such as Administrative, Preferences for

Customary Routine Activities, Active Diagnoses, Health Conditions, Medications, and Skin Conditions. We propose that HOPE data would be collected by hospice staff for each patient admission at three distinct time points: admission, the hospice update visit (HUV), and discharge, as discussed in the PRA as well as sections IV. A of this proposed rule in which we discuss Collection of Information requirements and the Regulatory Impact Analysis. We propose the timepoint for the HOPE Update Visits (HUV), which is dependent on the patient's length of stay (LOS), is limited to a subset of HOPE items addressing clinical issues important to the care of hospice patients as updates to the hospice plan of care. We propose that HOPE data be collected at these timepoints during the hospice's routine clinical assessments, based on unique patient assessment visits and additional follow-up visits as needed. As further discussed in the proposed draft HOPE Guidance Manual and PRA, not all HOPE items would be required to be completed at every timepoint. These proposed time points could also be revised in future rulemaking.

We propose that HOPE data collection would be effective beginning on or after October 1, 2025 to support the proposed quality measures anticipated for public reporting on or after CY 2027. After HOPE implementation, hospices would no longer need to collect and submit the Hospice Item Set (HIS). Additional details regarding the data collection required for the new HOPE item set are discussed below in section III. D6, Form, Manner, and Timing of Quality Measure Data Submission, and section IV., Collection of Information.

We propose to update § 418.312(a)(b)(1) to require hospices to complete and submit a standardized set of items for each patient to capture patient-level data, regardless of payer or patient age. This proposed change is intended to take effect October 1, 2025. This update will replace the previous requirement for hospices to complete the HIS and the newly standardized set of items would have to be completed at admission and discharge, and at the two HUV timepoints within the first 30 days after the hospice election. We note that, as authorized under section 1814(i)(5) of the Act, CMS would impose a 4 percent reduction on hospices for failure to submit HOPE collections timely with respect to that FY.

CMS is committed to ensuring hospices are ready for the proposed data collection beginning on or after October 1, 2025. We propose to provide information about upcoming provider trainings related to HOPE v1.0 that will

be posted on the *CMS HQRP website* on the *Announcement and Spotlight* page and announced during Open Door Forums. Past trainings about the HQRP are available through the *HQRP Training and Education Library*. These trainings will help providers understand the requirements necessary to be successful with the HQRP, including how data collected via the new draft HOPE tool is submitted for quality measures and contributes to compliance with the HQRP.

The draft HOPE Guidance Manual v1.0 is available on the HQRP HOPE web page for review and the final HOPE Guidance Manual v1.0 will be available after the publication of the final rule. This guidance manual offers hospices direction on the collection and submission of hospice patient stay data to CMS to support the HQRP quality measures.

Public Availability of Data Submitted

Under section 1814(i)(5)(E) of the Act, the Secretary is required to establish procedures for making any quality measure data submitted by hospices available to the public. The procedures ensure that a hospice will have the opportunity to review the data regarding the hospice's respective program before it is made public. In addition, under section 1814(i)(5)(E) of the Act, the Secretary is authorized to report data collected to support quality measures under section 1814(i)(5)(C) of the Act on the CMS website, that relate to services furnished by a hospice. We recognize that public reporting of quality measure data is a vital component of a robust quality reporting program and are fully committed to developing the necessary systems for public reporting of hospice quality measure data. We also recognize it is essential that the data made available to the public be meaningful and that comparing performance between hospices requires that measures be constructed from data collected in a standardized and uniform manner. The development and implementation of a standardized data set for hospices should precede public reporting of hospice quality measures. Once hospices have implemented the standardized data collection approach, we will have the data needed to establish the scientific soundness of the quality measures that can be calculated using the standardized data. It is critical to establish the reliability and validity of the measures prior to public reporting in order to demonstrate the ability of the measures to distinguish the quality of services provided. To establish reliability and validity of the quality measures, at least four quarters of data

will need to be analyzed. Typically, the first two quarters of data reflect the learning curve of the providers as they adopt a standardized data collection; these data are not used to establish reliability and validity. We propose that the data from the first quarter (anticipated to be Q4 CY2025, if HOPE data collection begins in October 2025) will not be used for assessing validity and reliability of the quality measures.

We propose to assess the quality and completeness of the data that we receive as we near the end of Q4 2025 before public reporting the measures. Data collected by hospices during the four quarters of CY 2026 (for example, Q 1, 2, 3 and 4 CY 2026) will be analyzed starting in CY 2027. We propose to inform the public of the decisions about whether to report some or all of the quality measures publicly based on the findings of analysis of the CY 2026 data.

In addition, as noted, the Affordable Care Act requires that reporting on the quality measures adopted under section 1814(i)(5)(D) of the Act be made public on a CMS website and that providers have an opportunity to review their data prior to public reporting. In light of all the steps required prior to data being publicly reported, we propose that public reporting of the proposed quality measures will be implemented no earlier than FY 2027. Alternatively, we propose public reporting may occur during the FY 2028 APU year, allowing ample time for data analysis, review of measures' appropriateness for use for public reporting, and allowing hospices the required time to review their own data prior to public reporting.

CMS will consider public reporting using fewer than four (4) quarters of data for the initial reporting period, but we propose to use 4 quarters of data as the standard reporting period for future public reporting. If the initial reporting period would include any excluded quarters of data, we propose to use as many non-excluded quarters of data as are included in the reporting period for public reporting. For example, if the first reporting period includes Q4 2024 2025 through Q3 2025 2026, then public reporting of HOPE will be based on Q1 2025 2026, Q2 2025 2026, and Q3 2025 2026. The next public reporting period would include Q1 2025 2026–Q4 2025 2026, and public reporting would be based on four (4) quarters of data, as would all subsequent rolling reporting periods.

We will propose the timeline for public reporting of data in future rulemaking and we welcome public comment on what we should consider when developing future proposals related to public reporting.

4. Health Equity Updates Related to HQRP

a. Background

Universal Foundation

To further the goals of the CMS National Quality Strategy (NQS), CMS leaders from across the Agency have come together to move towards a building-block approach to streamline quality measures across CMS quality programs for the adult and pediatric populations. We believe that this "Universal Foundation" of quality measures will focus provider attention, reduce burden, identify disparities in care, prioritize development of interoperable, digital quality measures, allow for cross-comparisons across programs, and help identify measurement gaps. The development and implementation of the Preliminary Adult and Pediatric Universal Foundation Measures will promote the best, safest, and most equitable care for individuals. As CMS moves forward with the Universal Foundation, we will be working to identify foundational measures in other specific settings and populations to support further measure alignment across CMS programs as applicable.

TEP Recommendations

In November and December 2022, CMS convened a group of stakeholders to provide input on the health equity measure development process. This HQRP and HH QRP Health Equity Structural Composite Measure Development Technical Expert Panel (or Home Health & Hospice HE TEP) included health equity experts from hospice and home health settings specializing in quality assurance, patient advocacy, clinical work, and measure development.

The TEP largely supported the potential health equity measure domains of Equity as a Key Organizational Priority, Trainings for Health Equity, and Organizational Culture of Equity. The TEP also recommended that CMS not only measure equity in service provision, but also equity in access to services. TEP members raised concerns about collecting hospice quality measure data from family or caregivers of hospice decedents rather than collecting data directly from patients while they are receiving care. Vulnerable populations without contacts post-mortem may be left out of data collection, such as hospice patients who do not have family members to help with their care or unhoused people. This feedback highlighted the importance of including SDOH such as housing instability in

hospice quality reporting. Hospice TEP members also recommended adding specific questions to the CAHPS® survey about cultural sensitivity.

Additional information regarding the Home Health & Hospice HE TEP are available in the TEP Report, available on the Hospice QRP Health Equity web page: <https://www.cms.gov/medicare/quality/hospice/hospice-grp-health-equity>.

b. Request for Information (RFI) Regarding Future HQRP Social Determinants of Health (SDOH) Items

CMS is committed to developing approaches to meaningfully incorporate the advancement of health equity into the HQRP. One consideration is including social determinants of health (SDOH) into our quality measures and data stratification. SDOH are the socioeconomic, cultural, and environmental circumstances in which individuals live that impact their health. SDOH can be grouped into five broad domains: economic stability; education access and quality; health care access and quality; neighborhood and built environment; and social and community context. Health-related social needs (HRSNs) are the resulting effects of SDOH, which are individual-level, adverse social conditions that negatively impact a person's health or health care. Examples of HRSN include lack of access to food, housing, or transportation, and have been associated with poorer health outcomes, greater use of emergency departments and hospitals, and higher health care costs. Certain HRSNs can lead to unmet social needs that directly influence an individual's physical, psychosocial, and functional status. This is particularly true for food security, housing stability, utilities security, and access to transportation. In recent years, we have addressed SDOH through the identification and standardization of screening for HRSN, including finalizing several standardized patient assessment data requirements for post-acute care providers⁷ and testing the

⁷ See the "Medicare and Medicaid Programs: CY 2020 Home Health Prospective Payment System Rate Update; Home Health Value-Based Purchasing Model; Home Health Quality Reporting Requirements; and Home Infusion Therapy Requirements" final rule (84 FR 39151) as an example. In the interim final rule with comment period (IFC) "Medicare and Medicaid Programs, Basic Health Program and Exchanges; Additional Policy and Regulatory Revisions in Response to the COVID-19 Public Health Emergency and Delay of Certain Reporting Requirements for the Skilled Nursing Facility Quality Reporting Program" (85 FR 27550 through 27629), CMS delayed the compliance dates for these standardized patient assessment data under the Inpatient Rehabilitation

Accountable Health Communities (AHC) model under section 1115A of the Social Security Act.⁸

We have repeatedly heard from the public that CMS should develop new HQRP mechanisms to better address significant and persistent health care outcome inequities. For example, in the FY 2022 Hospice Wage Index final rule, we received comments supportive of gathering standardized patient assessment data elements and additional SDOH data to improve health equity. In the FY 2023 Hospice final rule, we again received comments highlighting the need for more sociodemographic and SDOH data to effectively evaluate health equity in hospice settings. Commenters suggested that CMS consider standardizing the sociodemographic and SDOH data collected across provider settings and across third party vendors (for example, EMRs) and other tools. To this end, CMS expects to seek endorsement under 1890(a) for measures that would utilize SDOH data, within HQRP.

We are committed to achieving health equity in health care outcomes for our beneficiaries, including by improving data collection to better measure and analyze disparities across programs and policies.⁹ We believe that the ongoing measurement of SDOHs will have two significant benefits. First, because SDOHs disproportionately impact underserved communities, promoting

Facility (IRF) Quality Reporting Program (QRP), Long-Term Care Hospital (LTCH) QRP, Skilled Nursing Facility (SNF) QRP, and the Home Health (HH) QRP due to the public health emergency. In the “CY 2022 Home Health Prospective Payment System Rate Update; Home Health Value-Based Purchasing Model Requirements and Model Expansion; Home Health and Other Quality Reporting Program Requirements; Home Infusion Therapy Services Requirements; Survey and Enforcement Requirements for Hospice Programs; Medicare Provider Enrollment Requirements; and COVID-19 Reporting Requirements for Long-Term Care Facilities” final rule (86 FR 62240 through 62431), CMS finalized its proposals to require collection of standardized patient assessment data under the IRF QRP and LTCH QRP effective October 1, 2022, and January 1, 2023, for the HH QRP.

⁸ The Accountable Health Communities Model is a nationwide initiative established by the Center for Medicare and Medicaid Innovation Center to test innovative payment and service delivery models that have the potential to reduce Medicare, Medicaid, and Children’s Health Insurance Program expenditures while maintaining or enhancing the quality of beneficiaries care and was based on emerging evidence that addressing health-related social needs through enhanced clinical-community linkages can improve health outcomes and reduce costs. More information can be found at: <https://www.cms.gov/priorities/innovation/innovation-models/ahcm>.

⁹ Centers for Medicare & Medicaid Services. CMS Quality Strategy. 2016. <https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/QualityInitiativesGenInfo/Downloads/CMS-Quality-Strategy.pdf>.

measurement of these factors may serve as evidence-based building blocks for supporting healthcare providers and health systems in actualizing commitment to address disparities, improving health equity through addressing the social needs with community partners, and implementing associated equity measures to track progress.¹⁰ By measuring patient SDOH providers would be better equipped to identify disparities in patient populations and health outcomes. Better SDOH quality measures would serve as evidence-based building blocks for informing more effective programs to target and mitigate disparities, thereby enabling providers to improve patient outcomes.

Second, these factors could support ongoing HQRP initiatives by providing data with which to measure stratified resident risk and organizational performance. Further, we believe measuring resident-level SDOH through screening is essential in the long-term in encouraging meaningful collaboration between healthcare providers and community-based organizations, as well as in implementing and evaluating related innovations in health and social care delivery. Analysis of SDOH measures could allow providers to more effectively identify patient needs and identify opportunities for effective partnership with community-based organizations with the capacity to help address those needs. Thorough SDOH measures would also provide a better evidence base for evaluating the effectiveness and appropriateness of health and social care delivery innovations. The SDOH category of standardized patient assessment data elements could provide hospices and policymakers with meaningful measures as we seek to reduce disparities and improve care for beneficiaries with social risk factors. SDOH measures would also permit us to develop the statistical tools necessary to reduce costs and improve the quality of care for all beneficiaries. We note that advancing health equity by addressing the health disparities that underlie the country’s health system is one of our strategic pillars¹¹ and a Biden-Harris

¹⁰ American Hospital Association. (2020). Health Equity, Diversity & Inclusion Measures for Hospitals and Health System Dashboards. December 2020. Accessed: January 18, 2022. Available at: https://ifdhe.aha.org/system/files/media/file/2020/12/ifdhe_inclusion_dashboard.pdf.

¹¹ Brooks-LaSure, C. (2021). My First 100 Days and Where We Go from Here: A Strategic Vision for CMS. Centers for Medicare & Medicaid. Available at: <https://www.cms.gov/blog/my-first-100-days-and-where-we-go-here-strategic-vision-cms>.

Administration priority.¹² As such, CMS is working toward collecting SDOH data elements in hospice in support of quality measurement and seeks public comment on these efforts.

CMS reviewed SDOH domains to determine which domains align across post-acute care (PAC) and hospice care settings, circumstances, and setting-specific care goals. CMS identified four SDOH domains that are relevant across the PAC and hospice care setting: housing instability, food insecurity, utility challenges, and barriers to transportation access. These data elements have supported measures of quality in other settings. For example, as of 2023 the Hospital Inpatient Quality Reporting Program mandates reporting on the “Screening for Social Drivers of Health” and “Screen Positive Rate for Social Drivers of Health” measures.

CMS requests input on which of the data collection items outlined below are suitable for the hospice setting, and how they may need to be adapted to be more appropriate for the hospice setting.

Housing Instability

Healthy People 2030 prioritizes economic stability as a key SDOH, of which housing stability is a component.^{13 14} Lack of housing stability encompasses several challenges, such as having trouble paying rent, overcrowding, moving frequently, or spending the bulk of household income on housing.¹⁵ These experiences may negatively affect physical health and make it harder to access health care. Lack of housing stability can also lead to homelessness, which is housing deprivation in its most severe form. Homelessness is defined as “lacking a regular nighttime residence or having a primary nighttime residence that is a temporary shelter or other place not designed for sleeping.”¹⁶ On a single night in 2023, roughly 653,100 people, or 20 out of every 10,000 people in the United States, were experiencing

¹² The White House. The Biden-Harris Administration Immediate Priorities [website]. <https://www.whitehouse.gov/priorities/>.

¹³ <https://health.gov/healthypeople/priority-areas/social-determinants-health>.

¹⁴ Healthy People 2030 is a long-term, evidence-based effort led by the U.S. Department of Health and Human Services (HHS) that aims to identify nationwide health improvement priorities and improve the health of all Americans.

¹⁵ Kushel, M.B., Gupta, R., Gee, L., & Haas, J.S. (2006). Housing instability and food insecurity as barriers to health care among low-income Americans. *Journal of General Internal Medicine*, 21(1), 71–77. doi: 10.1111/j.1525-1497.2005.00278.x.

¹⁶ <https://health.gov/healthypeople/priority-areas/social-determinants-health/literature-summaries/housing-instability>.

homelessness.¹⁷ Studies also found that newly homeless people have an increased risk of premature death and

experience chronic disease more often than among the general population. The following options were identified as potential complimentary items to

collect housing information, in addition to proposed HOPE item A1905—Living Arrangements.

Exhibit I. Potential Items to Screen for Housing Instability in Hospice

Tool	Item	Response Options	Source
Accountable Health Communities Health Related Social Needs (AHC HRSN)	Think about the place you live. Do you have problems with any of the following?	a. Pests such as bugs, ants, or mice b. Mold c. Lead paint or pipes d. Lack of heat e. Oven or stove not working f. Smoke detectors missing or not working g. Water leaks h. None of the above	https://www.cms.gov/priorities/innovation/files/workshets/ahcm-screeningtool.pdf
Protocol for Responding to & Assessing Patients' Assets, Risks & Experience	Are you worried about losing your housing?	a. Yes b. No c. I choose not to answer this question	https://prapare.org/wp-content/uploads/2023/01/PRA-PARE-English.pdf

Food Insecurity

The U.S. Department of Agriculture, Economic Research Service defines a lack of food security as a household-level economic and social condition of limited or uncertain access to adequate food.¹⁸ Food insecurity has been a priority for the Biden-Harris Administration, with the White House recently announcing 141 stakeholder funding commitments to support the White House Challenge to End Hunger and Build Healthy Communities.¹⁹ Adults who are food insecure may be at an increased risk for a variety of

negative health outcomes and health disparities. For example, a study found that food-insecure adults may be at an increased risk for obesity.²⁰ Nutrition security is also an important component that builds on and complements long standing efforts to advance food security. The United States Department of Agriculture (USDA) defines nutrition security as “consistent and equitable access to healthy, safe, affordable foods essential to optimal health and well-being.”²¹ While having enough food is one of many predictors for health outcomes, a diet low in nutritious foods is also a factor.²² Studies have shown

that older adults struggling with food security consume fewer calories and nutrients and have lower overall dietary quality than those who are food secure, which can put them at nutritional risk. Older adults are also at a higher risk of developing malnutrition, which is considered a state of deficit, excess, or imbalance in protein, energy, or other nutrients that adversely impacts an individual’s own body form, function, and clinical outcomes. About 50 percent of older adults are affected by malnutrition, which is further aggravated by a lack of food security and poverty.²³

¹⁷ The 2023 Annual Homeless Assessment Report (AHAR) to Congress. The U.S. Department of Housing and Urban Development 2023. <https://www.huduser.gov/portal/sites/default/files/pdf/2023-AHAR-Part-1.pdf>.

¹⁸ U.S. Department of Agriculture, Economic Research Service. (n.d.). *Definitions of food security*. Retrieved March 10, 2022, from <https://www.ers.usda.gov/topics/food-nutrition-assistance/food-security-in-the-u-s/definitions-of-food-security/>.

¹⁹ <https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/27/fact-sheet-the-biden-harris-administration-announces-nearly-1-7-billion-in-new-commitments-cultivated-through-the-white-house-challenge-to-end-hunger-and-build-healthy-communities/>.

²⁰ Hernandez, D.C., Reesor, L.M., & Murillo, R. (2017). Food insecurity and adult overweight/obesity: Gender and race/ethnic disparities. *Appetite*, 117, 373–378.

²¹ Food and Nutrition Security. (n.d.). USDA. <https://www.usda.gov/nutrition-security>.

²² National Center for Health Statistics. (2022, September 6). Exercise or Physical Activity. Retrieved from Centers for Disease Control and Prevention: <https://www.cdc.gov/nchs/fastats/exercise.htm>.

²³ Food Research & Action Center (FRAC). “Hunger is a Health Issue for Older Adults: Food Security, Health, and the Federal Nutrition Programs.” December 2019. <https://frac.org/wp-content/uploads/hunger-is-a-health-issue-for-older-adults-1.pdf>.

Exhibit II. Potential Items to Screen for Food Insecurity in Hospice

Tool	Item	Response Options	Source
Health Begins - Upstream Risk Screening Tool	Which of the following describes the amount of food your household has to eat: (Check one.)	a. Enough to eat b. Sometimes not enough to eat c. Often not enough to eat	https://www.aamc.org/media/25736/download
Hunger Vital Sign	1. Within the past 12 months we worried whether our food would run out before we got money to buy more.	a. Often true b. Sometimes true c. Never true	https://childrenshealthwatch.org/public-policy/hunger-vital-sign/
	2. Within the past 12 months the food we bought just didn't last and we didn't have money to get more.	a. Often true b. Sometimes true c. Never true	
Children's HealthWatch	In the past year, have you ever used a Food Pantry/Soup Kitchen or received a food donation?	Yes No	http://childrenshealthwatch.org/public-policy/hunger-vital-sign/

Utility Challenges

A lack of energy (utility) security can be defined as an inability to adequately meet basic household energy needs.²⁴ According to the Department of Energy, one in three households in the US are unable to adequately meet basic household energy needs.²⁵ The consequences associated with a lack of utility security are represented by three primary dimensions: economic, physical, and behavioral. Individuals with low incomes are disproportionately affected by high energy costs, and they may be forced to prioritize paying for housing and food over utilities. Some people may face

limited housing options and are at increased risk of living in lower-quality physical conditions with malfunctioning heating and cooling systems, poor lighting, and outdated plumbing and electrical systems. Finally, individuals who lack of utility security may use negative behavioral approaches to cope, such as using stoves and space heaters for heat.²⁶ In addition, data from the Department of Energy's US Energy Information Administration confirm that a lack of energy security disproportionately affects certain populations, such as low-income and African American households.²⁷ The effects of a lack of utility security include vulnerability to environmental

exposures such as dampness, mold, and thermal discomfort in the home, which have direct effect on residents' health. For example, research has shown associations between a lack of energy security and respiratory conditions as well as mental health-related disparities and poor sleep quality in vulnerable populations such as the elderly, children, the socioeconomically disadvantaged, and the medically vulnerable.²⁸ Adopting a data element to collect information about utility security across PAC settings could facilitate the identification of residents who may not have utility security and who may benefit from engagement efforts.

²⁴ Hernández D. Understanding 'energy insecurity' and why it matters to health. Soc Sci Med. 2016 Oct; 167:1–10. doi: 10.1016/j.socscimed.2016.08.029. Epub 2016 Aug 21. PMID: 27592003; PMCID: PMC5114037.

²⁵ U.S. Energy Information Administration. "One in Three U.S. Households Faced Challenges in Paying Energy Bills in 2015." 2017 Oct 13. <https://www.eia.gov/consumption/residential/reports/2015/energybills/>.

www.eia.gov/consumption/residential/reports/2015/energybills/.

²⁶ Hernández D. "What 'Merle' Taught Me About Energy Insecurity and Health." Health Affairs, VOL.37, NO.3: Advancing Health Equity Narrative Matters. March 2018. <https://doi.org/10.1377/hlthaff.2017.1413>.

²⁷ US Energy Information Administration. "One in Three U.S. Households Faced Challenges in Paying Energy Bills in 2015." 2017 Oct 13. <https://www.eia.gov/consumption/residential/reports/2015/energybills/>.

²⁸ Hernández D. "Understanding 'energy insecurity' and why it matters to health." Soc Sci Med. 2016; 167:1–10.

Exhibit III. Potential Items to Screen for Utility Challenges in Hospice

Tool	Item	Response Options	Source
North Carolina Medicaid Screening Tool	Within the past 12 months, have you been unable to get utilities (heat, electricity) when it was really needed?	Yes No	https://www.ncdhhs.gov/about/department-initiatives/healthy-opportunities/screening-questions
WELL RX Toolkit	Do you have trouble paying for your utilities (gas, electricity, phone)?	Yes No	https://sirenetwork.ucsf.edu/tools-resources/resources/wellrx-toolkit
Health Leads - Social Needs Screening Toolkit	In the last 12 months, has the electric, gas, oil, or water company threatened to shut off your services in your home?	Yes No	https://healthleadsusa.org/wp-content/uploads/2023/05/Screening_Toolkit_2018.pdf

Transportation Challenges

Transportation barriers can both directly and indirectly affect a person's health. A lack of transportation can keep

patients from accessing medical appointments, getting medications, or from getting things they need daily. It can also affect a person's health by creating a barrier to accessing goods and

services, obtaining adequate food and clothing, or attending social activities. Therefore, reliable transportation services are fundamental to a person's health.

Exhibit IV. Potential Items to Screen for Transportation Challenges in Hospice

Tool	Item	Response Options	Source
AHC HRSN	In the past 12 months, has lack of reliable transportation kept you from medical appointments, meetings, work or from getting things needed for daily living?	Yes No	https://www.cms.gov/priorities/innovation/files/worksheets/a-hcm-screeningtool.pdf
Borders	Are you regularly able to get a friend or relative to take you to doctor's appointments?	Yes No	https://oaktrust.library.tamu.edu/bitstream/handle/1969.1/6016/etd-tamu-2006A-URSC-Borders.pdf

All Domains

Exhibit V. Potential Items to Screen for All Domains

Tool	Item	Response Options	Source
Kaiser Permanente's Your Current Life Situation Survey	In the past 3 months, did you have trouble paying for any of the following?	a. Food b. Housing c. Heat and electricity d. Medical needs e. Transportation f. Childcare g. Debts h. Other i. None of these	https://sirenetwork.ucsf.edu/sites/default/files/Your%20Current%20Life%20Situation%20Questionnaire%20v2%20-%20Core%20and%20supplemental%29%20no%20highlights.pdf

We solicit public comment on the following questions:

- For each of the domains:
 - ++ Are these items relevant for hospice patients? Are these items relevant for hospice caregivers?
 - ++ Which of these items are most suitable for hospice?
 - ++ How might the items need to be adapted to improve relevance for hospice patients and their caregivers? Would you recommend adjusting the listed timeframes for any items? Would you recommend revising any of the items' response options?
- Are there additional SDOH domains that would also be useful for identifying and addressing health equity issues in Hospice?

5. Proposed CAHPS Hospice Survey and Measure Changes

a. Survey and Measure Changes

In the Fiscal Year 2024 Hospice Payment Rate Update Final Rule (88 FR 51164), CMS provided the results of a mode experiment conducted with 56 large hospices in 2021. The experiment tested a web-mail mode, modification to survey administration protocols such as adding a prenotification letter and extending the data collection period, and a revised survey version. Because we believe the results of the experiment were successful, we are proposing changes to the CAHPS Hospice Survey and administrative protocol. The revised survey is shorter and simpler than the current survey and includes new questions on topics suggested by stakeholders. Specifically, proposed

changes to the survey and the quality measures derived from testing include:

- Removal of three nursing home items and an item about moving the family member²⁹ that are not included in scored measures.
- Removal of one survey item regarding confusing or contradictory information from the Hospice Team Communication measure.³⁰
- Replacement of the multi-item Getting Hospice Care Training measure³¹ with a new, one-item summary measure.
- Addition of two new items, which will be used to calculate a new Care Preferences measure.
- Simplified wording to component items in the Hospice Team Communication, Getting Timely Care, and Treating Family Member with Respect measures.

The revised CAHPS Hospice Survey, including the new Care Preferences measure, the revised Hospice Team Communication measure, and the revised Getting Hospice Care Training measure received endorsement through the Consensus Standards Approval Committee (CSAC) Fall 2022 endorsement and maintenance cycle. Recommendations from the endorsement committee resulted in edits to the Getting Emotional and Religious Support to reflect cultural needs.

The Care Preferences, Hospice Team Communication, and Getting Hospice Care Training measures are on the 2023 Measures Under Consideration list (MUC2023–183,191 & 192) and are under evaluation by the Pre-Rulemaking

Measure Review (PRMR) Post-Acute Care/Long-Term Care (PAC/LTC) Committee. The Consensus-Based Entity (CBE) utilizes the Novel Hybrid Delphi and Nominal Group (NHDNG) multi-step process, which is an iterative consensus-building approach aimed at a minimum of 75 percent agreement among voting members, rather than a simple majority vote, and supports maximizing the time spent to build consensus by focusing discussion on measures where there is disagreement. The final result from the committee's vote can be: "Recommend", "Recommend with conditions", "Do not recommend" or "Consensus not reached". "Consensus not reached" signals continued disagreement amongst the committee despite being presented with perspectives from public comment, committee member feedback and discussion, and highlights the multifaceted assessments of quality measures. The CBE did not reach consensus on the CAHPS Hospice Survey measures. More details regarding the CBE Pre-Rulemaking Measure Review (PRMR) voting procedures may be found in Chapter 4 of the Guidebook of Policies and Procedures for Pre-Rulemaking Measure Review and Measure Set Review.

CMS is proposing to implement the revised CAHPS Hospice Survey beginning with January 2025 decedents. Table 14 provides a comparison of the current and proposed CAHPS Hospice Survey measures.

BILLING CODE 4120-01-P

²⁹The current version of the CAHPS Hospice Survey is available at: <https://hospicecahpsurvey.org/en/survey-materials/>. The proposed items are for removal from this version of the survey are: Question 32 through 34 (nursing

home items), Question 30 (item about moving a family member), Question 10 (item regarding confusing or contradictory information), and Question 17 through 20, 23, 28, and 29 (screening

and evaluative items used to calculate the Getting Hospice Care Training measure).

³⁰Ibid.

³¹Ibid.

TABLE 14: Comparison of Current and Proposed CAHPS Hospice Survey Measures

Measure	Item(s) in Current Measure	Item(s) in Proposed Revised or New Measure
Getting Timely Care	“How often did you get the help you needed from the hospice team during evenings, weekends, or holidays?”	“How often did you get the help you needed from the hospice team during evenings, weekends, or holidays?”
	“While your family member was in hospice care, when you or your family member asked for help from the hospice team, how often did you get help as soon as you needed it?”	“When you or your family member asked for help from the hospice team, how often did you get help as soon as you needed it?”
Hospice Team Communication	“While your family member was in hospice care, how often did the hospice team keep you informed about when they would arrive to care for your family member?”	“How often did the hospice team let you know when they would arrive to care for your family member?”
	“While your family member was in hospice care, how often did the hospice team explain things in a way that was easy to understand?”	“How often did the hospice team explain things in a way that was easy to understand?”
	“While your family member was in hospice care, how often did the hospice team keep you informed	“How often did the hospice team keep you informed about your family member’s condition?”

Measure	Item(s) in Current Measure	Item(s) in Proposed Revised or New Measure
	about your family member's condition?"	
	"While your family member was in hospice care, how often did anyone from the hospice team give you confusing or contradictory information about your family member's condition or care?"	N/A (removed from revised survey)
	"How often did the hospice team listen carefully to you when you talked with them about problems with your family member's hospice care?"	"How often did the hospice team listen carefully to you when you talked with them about problems with your family member's hospice care?"
	"While your family member was in hospice care, how often did the hospice team listen carefully to you?"	"While your family member was in hospice care, how often did the hospice team listen carefully to you?"
Treating Family Member with Respect	"While your family member was in hospice care, how often did the hospice team treat your family member with dignity and respect?"	"How often did the hospice team treat your family member with dignity and respect?"
	"While your family member was in hospice care, how often did you	"How often did you feel that the hospice team really cared about

Measure	Item(s) in Current Measure	Item(s) in Proposed Revised or New Measure
	feel that the hospice team really cared about your family member?"	your family member?"
Getting Help for Symptoms	"Did your family member get as much help with pain as he or she needed?"	"Did your family member get as much help with pain as they needed?"
	"How often did your family member get the help he or she needed for trouble breathing?"	"How often did your family member get the help they needed for trouble breathing?"
	"How often did your family member get the help he or she needed for trouble with constipation?"	"How often did your family member get the help they needed for trouble with constipation?"
	"How often did your family member get the help he or she needed <u>from the hospice team</u> for feelings of anxiety or sadness?"	"How often did your family member get the help they needed <u>from the hospice team</u> for feelings of anxiety or sadness?"
Getting Emotional and Religious Support	"Support for religious or spiritual beliefs includes talking, praying, quiet time, or other ways of meeting your religious or spiritual needs. While your family member was in hospice care, how much support for your religious and	"Support for religious, spiritual, or cultural beliefs may include talking, praying, quiet time, and respecting traditions. While your family member was in hospice care, how much support for your religious, spiritual, and cultural beliefs did

Measure	Item(s) in Current Measure	Item(s) in Proposed Revised or New Measure
	spiritual beliefs did you get from the hospice team?"	you get from the hospice team?"
	"While your family member was in hospice care, how much emotional support did you get from the hospice team?"	"While your family member was in hospice care, how much emotional support did you get from the hospice team?"
	"In the weeks <u>after</u> your family member died, how much emotional support did you get from the hospice team?"	"In the weeks <u>after</u> your family member died, how much emotional support did you get from the hospice team?"
Getting Hospice Care Training	"Side effects of pain medicine include things like sleepiness. Did any member of the hospice team discuss side effects of pain medicine with you or your family member?"	N/A (removed from revised survey)
	"Did the hospice team give you the training you needed about what side effects to watch for from pain medicine?"	N/A (removed from revised survey)
	"Did the hospice team give you the training you needed about if and when to give more pain medicine to	N/A (removed from revised survey)

Measure	Item(s) in Current Measure	Item(s) in Proposed Revised or New Measure
	your family member?"	
	"Did the hospice team give you the training you needed about how to help your family member if he or she had trouble breathing?"	N/A (removed from revised survey)
	"Did the hospice team give you the training you needed about what to do if your family member became restless or agitated?"	N/A (removed from revised survey)
	N/A (not on current survey)	"Hospice teams may teach you how to care for family members who need pain medicine, have trouble breathing, are restless or agitated, or have other care needs. Did the hospice team teach you how to care for your family member?"
Care preferences	N/A (not on current survey)	"Did the hospice team make an effort to listen to the things that mattered most to you or your family member?"
	N/A (not on current survey)	"Did the hospice team provide care that respected your family member's wishes?"

Measure	Item(s) in Current Measure	Item(s) in Proposed Revised or New Measure
Overall rating	“Please answer the following questions about your family member’s care from the hospice named on the survey cover. Do not include care from other hospices in your answers. Using any number from 0 to 10, where 0 is the worst hospice care possible and 10 is the best hospice care possible, what number would you use to rate your family member’s hospice care?”	“Please answer the following questions about the hospice named on the survey cover. Do not include care from other hospices in your answers. Using any number from 0 to 10, where 0 is the worst hospice care possible and 10 is the best hospice care possible, what number would you use to rate your family member’s hospice care?”
Willingness to recommend	“Would you recommend this hospice to your friends and family?”	“Would you recommend this hospice to your friends and family?”

BILLING CODE 4120-01-C

We seek comment on these proposed changes before finalization.

b. Impact to Public Reporting and Star Ratings

CAHPS Hospice Survey measure scores are calculated across eight rolling quarters and are published quarterly for all hospices with 30 or more completed surveys over the reporting period. The Family Caregiver Survey Rating summary Star Rating is also calculated using eight rolling quarters and is publicly reported for all hospices with 75 or more completed surveys over the reporting period. Star Ratings are updated every other quarter. To determine what impact the changes to the survey measures would have on public reporting, CMS considered the nature of the measure change. As “Care

Preferences” would be a new measure for the CAHPS Hospice Survey, we would have to wait to introduce public reporting until we have eight quarters of data. Although the revised “Getting Hospice Care Training” measure would be conceptually similar to the current “Getting Hospice Care Training” measure, we believe the change (one summary item instead of several items) is substantive and the revised measure should be treated as new for purposes of public reporting and Star Ratings. As such, we propose waiting to publicly report the new version of “Getting Hospice Care Training” until we have eight quarters of data. We anticipate that the first Care Compare refresh in which publicly reported measures scores would be updated to include the new measures would be November 2027,

with scores calculated using data from Q1 2025 through Q4 2026. Because measure scores are calculated quarterly and Star Ratings are calculated every other quarter, these changes may be introduced in different quarters for measure scores and Star Ratings. In the interim period, measure scores would be made available to hospices confidentially in their Provider Preview reports once they met a threshold number of completed surveys.

We believe the proposed changes to the “Hospice Team Communication” measure (removing one item and slight wording changes) are non-substantive (that is, would not meaningfully change the measure) and that the measure could continue to be publicly reported and used in Star Ratings in the transition period between the current and new

surveys. During the transition period, scores and Star Ratings would be calculated by combining scores from quarters using the current and new survey. As a result of the survey measure changes, we propose that the Family Caregiver Survey Rating summary Star Rating will be based on seven measures rather than the current eight measures during the interim period until a full eight quarters of data are available for the “Getting Hospice Care Training” measure. The summary Star Rating would be based on nine measures once eight quarters of data are available for the new Care Preference and Getting Hospice Care Training measures.

c. Survey Administration Changes

CMS is proposing to add a web-mail mode (email invitation to a web survey, with mail follow-up to non-responders); to add a pre-notification letter; and to extend the field period from 42 to 49 days, beginning with January 2025 decedents. The 2021 mode experiment found increases to response rates with these changes to survey administrative protocols. The web-mail mode would be an alternative to the current modes (mail-only, telephone-only, and mixed mode (mail with telephone follow-up)) that hospices could select. In the mode experiment, among those with no available email addresses, response rates to the mail-only and web-mail modes were similar (35.2 percent vs. 34.3 percent); however, among those with available email addresses, adjusted response rates were substantially and significantly different—36.7 percent for mail-only versus 49.6 percent for web-mail—suggesting a notable benefit of the web-mail mode for hospices with available email addresses for some caregivers.

In the mode experiment, we found that mailing a pre-notification letter one week prior to survey administration was associated with an increase in response rates of 2.4 percentage points. We currently require a prenotification letter for the Medicare Advantage and Prescription Drug Plan and the In-center Hemodialysis CAHPS initiatives, so there is precedent for this requirement for CAHPS surveys, and mailing the letter is well within the capabilities of all approved survey vendors.

Currently, the CAHPS Hospice Survey is fielded over 42 days; responses that come in after the 42-day window are not included in analysis and scoring. Extending the field period by one week (to 49 days) is feasible within the current national implementation data collection and submission timeline. Our proposal to extend the field period to 49

days is estimated to result in an increased response rate of 2.5 percentage points in the mail-only mode, the predominant mode in which CAHPS Hospice Surveys are currently administered.

d. Case-Mix and Mode Adjustments

Prior to public reporting, hospices’ CAHPS Hospice Survey scores are adjusted for the effects of both mode of survey administration and case mix. Case mix refers to characteristics of the decedent and the caregiver that are not under control of the hospice that may affect reports of hospice experiences. Case-mix adjustment is performed within each quarter of data after data cleaning and mode adjustment. The current case-mix adjustment model includes the following variables: response percentile (the lag time between patient death and survey response), decedent’s age, payer for hospice care, decedent’s primary diagnosis, decedent’s length of final episode of hospice care, caregiver’s education, decedent’s relationship to caregiver, caregiver’s preferred language and language in which the survey was completed, and caregiver’s age. CMS reviewed the variables included in the case-mix adjustment models currently in use for the CAHPS Hospice Survey to determine if any changes needed to be introduced along with the revised survey and new mode. We found that no case-mix variables need to be added or removed.

With the introduction of a new mode of survey administration and survey items, CMS proposes updating the analytic adjustments that adjust responses for the effect of mode on survey responses. When we make mode adjustments, it is necessary to choose one mode as a reference mode. One can then interpret all adjusted responses from all modes as if they had been surveyed in the reference mode. Telephone-only is currently the reference mode for the CAHPS Hospice Survey. We are proposing to change the reference mode to mail-only. In the 2015 CAHPS Hospice Survey mode experiment, telephone-only respondents had consistently worse scores than mail-only respondents across measures. However, in the 2021 mode experiment, differences in scores between mail-only and telephone-only respondents were no longer in a consistent direction across measures. Given this, we are proposing to use mail-only as the reference mode beginning with January 2025 decedents as most surveys are currently completed in the mail-only mode. We invite public comment on the CAHPS Hospice Survey proposals.

6. Form, Manner, and Timing of Quality Measure Data Submission

a. Statutory Penalty for Failure To Report

Section 1814(i)(5)(C) of the Act requires that each hospice submit data to the Secretary on quality measures specified by the Secretary. The data must be submitted in a form and manner, and at a time specified by the Secretary. Section 1814(i)(5)(A)(i) of the Act was amended by the CAA, 2021 and the payment reduction for failing to meet hospice quality reporting requirements was increased from 2 percent to 4 percent beginning with FY 2024. During FYs 2014 through 2023, the Secretary reduced the market basket update by 2 percentage points for non-compliance. Beginning in FY 2024 and for each subsequent year, the Secretary will reduce the market basket update by 4 percentage points for any hospice that does not comply with the quality measure data submission requirements for that FY. In the FY 2023 Hospice Wage Index final rule (87 FR 45669), we revised our regulations at § 418.306(b)(2) in accordance with this statutory change (86 FR 42605).

b. HOPE Data Collection

Hospices will be required to begin collecting and submitting HOPE data as of October 1, 2025. After this effective date, hospices will no longer be required to collect or submit the Hospice Item Set (HIS).

We propose that hospices begin the use of HOPE in October 2025 and submit HOPE assessments to the CMS data submission and processing system in the required format designated by CMS (as set out in subregulatory guidance). At the time of implementation (that is, October 2025), all HOPE records would need to be submitted as an XML file, which is also the required format for the HIS. The format is subject to change in future years as technological advancements occur and healthcare provider use of electronic records increases, as well as systems become more interoperable.

We will provide the HOPE technical data specifications for software developers and vendors on the CMS website. Software developers and vendors should not wait for final technical data specifications to begin development of their own products. Rather, software developers and vendors are encouraged to thoroughly review the draft technical data specifications and provide feedback to CMS so we may address potential issues adequately and in a timely manner. We will conduct a call with software developers and

vendors after the draft specifications are posted, during which we will respond to questions, comments, and suggestions. This process will ensure software developers and vendors are successful in developing their products to better support the successful implementation of HOPE for all parties. Hospice providers will need to use vendor software to submit HOPE records to CMS. As with HIS, facilities that fail to submit all required HOPE assessments to CMS for at least 90% of their patients will be subject to a 4% reduction. See “Submission of Data Requirements” section below for additional information.

c. Retirement of Hospice Abstraction Reporting Tool (HART)

In 2014, CMS made a free tool (Hospice Abstraction Reporting Tool, or HART) available which providers could use to collect HIS data. Over time we observed that only a small percentage of hospices utilized the tool. Therefore, in

light of the limited utility the free tool provided, we will no longer provide a free tool for standardized data collection. Beginning October 1, 2025, hospices will need to select a private vendor to collect and submit HIS data, and subsequently HOPE data, to CMS.

d. Compliance

HQRP Compliance requires understanding three timeframes for both HIS and CAHPS: The relevant Reporting Year; the payment FY; and the Reference Year.

(1) The “Reporting Year” (HIS) or “Data Collection Year” (CAHPS) is based on the calendar year (CY). It is the same CY for both HIS (or HOPE, once it is implemented) and CAHPS. If the CAHPS Data Collection year is CY 2025, then the HIS (or HOPE) reporting year is also CY 2025.

(2) In the “Payment FY”, the APU is subsequently applied to FY payments based on compliance in the corresponding Reporting Year/Data Collection Year.

(3) For the CAHPS Hospice Survey, the Reference Year is the CY before the Data Collection Year. The Reference Year applies to hospices submitting a size exemption from the CAHPS survey (there is no similar exemption for HIS or HOPE). For example, for the CY 2025 data collection year, the Reference Year is CY 2024. This means providers seeking a size exemption for CAHPS in CY 2025 will base it on their hospice size in CY 2024.

Submission requirements are codified at 42 CFR 418.312. Table 15 summarizes the three timeframes. It illustrates how the CY interacts with the FY payments, covering the CY 2023 through CY 2026 data collection periods and the corresponding APU application from FY 2025 through FY 2028. Please note that during the first reporting year that implements HOPE, APUs may be based on fewer than four quarters of data. CMS will provide additional subregulatory guidance regarding APUs for the HOPE implementation year.

TABLE 15: HQRP Reporting Requirements and Corresponding Annual Payment Updates

Reporting Year for HIS/HOPE and Data Collection Year for CAHPS data (Calendar year)	Annual Payment Update Impacts Payments for the FY	Reference Year for CAHPS Size Exemption (CAHPS only)
CY 2023	FY 2025 APU	CY 2022
CY 2024	FY 2026 APU	CY 2023
CY 2025	FY 2027 APU	CY 2024
CY 2026	FY 2028 APU	CY 2025

As illustrated in Table 15 CY 2023 data submissions compliance impacts the FY 2025 APU. CY 2024 data submissions compliance impacts the FY 2026 APU. CY 2025 data submissions compliance impacts FY 2027 APU. This CY data submission impacting FY APU pattern follows for subsequent years.

e. Submission of Data Requirements

As finalized in the FY 2016 Hospice Wage Index final rule (80 FR 47142, 47192), hospices’ compliance with HIS requirements beginning with the FY 2020 APU determination (that is, based on HIS-Admission and Discharge records submitted in CY 2018) are based on a timeliness threshold of 90 percent. This means CMS requires that hospices submit 90 percent of all required HIS

records within 30 days of the event (that is, patient’s admission or discharge). The 90-percent threshold is hereafter referred to as the timeliness compliance threshold. Ninety percent of all required HIS records must be submitted and accepted within the 30-day submission deadline to avoid the statutorily-mandated payment penalty.

We propose to apply the same submission requirements for HOPE admission, discharge, and two HUV records. After HIS is phased out, hospices would continue to submit 90 percent of all required HOPE records to support the quality measures within 30 days of the event or completion date (patient’s admission, discharge, and based on the patient’s length of stay up to two HUV timepoints).

Hospice compliance with claims data requirements is based on administrative data collection. Since Medicare claims data are already collected from claims, hospices are considered 100 percent compliant with the submission of these data for the HQRP. There is no additional submission requirement for administrative data.

To comply with CMS’ quality reporting requirements for CAHPS, hospices are required to collect data monthly using the CAHPS Hospice Survey. Hospices comply by utilizing a CMS-approved third-party vendor. Approved Hospice CAHPS vendors must successfully submit data on the hospice’s behalf to the CAHPS Hospice Survey Data Center. A list of the approved vendors can be found on the

CAHPS Hospice Survey website:
www.hospicecahpsurvey.org.

Table 16. HQRP Compliance Checklist illustrates the APU and timeliness threshold requirements.

BILLING CODE 4120-01-P

TABLE 16: HQRP Compliance Checklist

Annual payment update	HIS/HOPE	CAHPS
FY 2025	Submit at least 90 percent of all HIS records within 30 days of the event date (for example patient's admission or discharge) for patient admissions/discharges occurring 1/1/23-12/31/23	Ongoing monthly participation in the Hospice CAHPS survey 1/1/2023-12/31/2023
FY 2026	Submit at least 90 percent of all HIS records within 30 days of the event date (for example, patient's admission or discharge) for patient admissions/discharges occurring 1/1/24-12/31/24	Ongoing monthly participation in the Hospice CAHPS survey 1/1/2024-12/31/2024
FY 2027	Submit at least 90 percent of all HIS/HOPE records within 30 days of the event date (for example, patient's admission or discharge) for patient admissions/discharges occurring 1/1/25-12/31/25	Ongoing monthly participation in the Hospice CAHPS survey 1/1/2025-12/31/2025
FY 2028	Submit at least 90 percent of all HIS/HOPE records within 30 days of the event or completion date (for example, patient's admission date, HUV completion date or discharge date) for patient admissions/discharges occurring 1/1/26-12/31/26	Ongoing monthly participation in the Hospice CAHPS survey 1/1/2026-12/31/2026

Note: The data source for the claims-based measures will be Medicare claims data that are already collected and submitted to CMS. There is no additional submission requirement for administrative data (Medicare claims), and hospices with claims data are 100-percent compliant with this requirement.

BILLING CODE 4120-01-C

Most hospices that fail to meet HQRP requirements do so because they miss the 90 percent threshold. We offer many training and education opportunities

through our website, which are available 24/7, 365 days per year, to enable hospice staff to learn at the pace and time of their choice. We want

hospices to be successful with meeting the HQRP requirements. We encourage hospices to use the website at: <https://www.cms.gov/Medicare/Quality->

Initiatives-Patient-Assessment-Instruments/Hospice-Quality-Reporting/Hospice-Quality-Reporting-Training-Training-and-Education-Library. For more information about HQRP Requirements, we refer readers to visit the frequently-updated HQRP website and especially the Requirements and Best Practice, Education and Training Library, and Help Desk web pages at: <https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/Hospice-Quality-Reporting>. We also encourage readers to visit the HQRP web page and sign-up for the Hospice Quality ListServ to stay informed about HQRP.

IV. Collection of Information Requirements

Under the Paperwork Reduction Act of 1995, we are required to provide 60-day notice in the **Federal Register** and solicit public comment before a collection of information requirement is submitted to the Office of Management and Budget (OMB) for review and approval. In order to fairly evaluate whether an information collection should be approved by OMB, section 3506(c)(2)(A) of the Paperwork

Reduction Act of 1995 requires that we solicit comment on the following issues:

- The need for the information collection and its usefulness in carrying out the proper functions of our agency.
- The accuracy of our estimate of the information collection burden.
- The quality, utility, and clarity of the information to be collected.
- Recommendations to minimize the information collection burden on the affected public, including automated collection techniques.

We are soliciting public comment on each of these issues for the following sections of this document that contain information collection requirements (ICRs):

A. Hospice Outcomes & Patient Evaluation (HOPE)

As proposed in section III. of this proposed rule, we are proposing the use of HOPE to collect QRP information through revisions to § 418.312(b). We are also proposing to require HOPE as a hospice patient-level item set to be used by all hospices to collect and submit standardized data on each patient admitted to hospice. HOPE would be used to support the

standardized collection of the requisite data elements to calculate quality measures being utilized by the QRP. Hospices would be required to complete and submit an admission HOPE and a discharge HOPE collecting a range of status data (set out in the PRA accompanying this Rule, as well as the HOPE Guidance Manual proposed in this Rule) for each patient, as well as a HOPE Update Visit assessment, when applicable, starting October 1, 2025, for FY 2027 APU determination.

CMS data indicates that approximately 5,640 hospices enroll approximately 2,763,850 patients in hospice annually.

According to the most recent wage data provided by the Bureau of Labor Statistics (BLS) for May 2022 (see http://www.bls.gov/oes/current/oes_nat.htm), the median hourly wage for Registered Nurses is \$39.05 and the mean hourly wage for Medical Secretaries is \$18.51. With fringe benefits and overhead, the total per hour rate for Registered Nurses is \$78.10, and the total per hour rate for Medical Secretaries is \$37.02. The foregoing wage figures are outlined in Table 17:

TABLE 17: National Occupational Employment and Wage Estimates

Occupation title	Occupation code	Median hourly wage (\$/hr)	Fringe benefits and overhead (\$/hr)	Adjusted hourly wage (\$/hr)
Registered Nurse	29-1141	\$39.05	\$39.05	\$78.10
Medical Secretary	43-6013	\$18.51	\$18.51	\$37.02

The annual time and cost burden for HOPE is calculated by determining the number of hours spent on each HOPE timepoint and using an average salary for nurses and medical secretaries to determine the average cost of the time spent on the assessment.

The total number of Medicare-participating hospices (5,640) and the total number of admissions per year (2,763,850) are gathered from claims data collected by CMS. Based on these claims data, we determined that there are approximately 490 admissions per hospice per year. We then use data from previous HIS item timings and HOPE beta testing to determine the average time to complete the three HOPE timepoints. The time-to-complete is then calculated for each HOPE

timepoint for nurses (clerical staff are assumed to take 5 minutes per timepoint to upload data). HOPE Admission is estimated to take 27 minutes for a nurse to complete relative to HIS, the new HOPE HUV is estimated to take 22 minutes for a nurse to complete, and HOPE Discharge is estimated to take 0 minutes to complete. Together, these burden increases represent a 54-minute increase per assessment (22 + 27 + 5 = 54 minutes). We also note that, due to the addition of the HUV timepoint, hospices will submit an estimated 2,763,850 additional HOPE assessments (one HUV assessment per admission).

By multiplying the average time-to-complete with the number of records for a timepoint, we determine the average

increase in burden hours spent for both nurses and clinical staff annually (Admission: 1,243,733 hours, HUV: 1,243,733 hours, Discharge: 0 hours). For additional information regarding the calculation of HOPE time and cost burdens, please refer to the HOPE Beta Testing Report found on the HOPE web page at <https://www.cms.gov/medicare/quality/hospice/hope> and the PRA package associated with this rule found at <https://www.cms.gov/medicare/regulations-guidance/legislation/paperwork-reduction-act-1995/pralisting>.

To calculate the cost burden, we multiply hospice staff wages by the amount of time those staff need to spend administering HOPE. We use the most recent hourly wage data for Registered

Nurses (\$39.05 per hour) and Medical Secretaries (\$18.51 per hour) from the U.S. Bureau of Labor Statistics. These wages are doubled to account for fringe benefits (\$78.10 for Registered Nurses, \$37.02 for Medical Secretaries). Nurse and Medical Secretary wages are then calculated separately by multiplying time spent on timepoints with the number of HOPE records with the average wages (for example: 49 clinical minute increase on HOPE × 490 HOPE records per year/60 minutes × \$78.10 = \$31,253.02 nursing wages spent per hospice per year). The calculations for each of these hospice staff disciplines

are added together to determine the total cost burden increase per hospice. Based on these calculations, we estimate that our proposal would therefore result in an incremental increase of 2,487,466-hour annual burden (1,243,733 hours for HOPE Admissions, 1,243,733 hours for HOPE Update Visits, and 0 hours for HOPE Discharges) at a cost of \$184,792,739. The total cost burden per hospice (\$32,764.67) is calculated by adding the total clinical cost (\$31,253.02, as seen above) with the total clerical staff cost burden (5 minutes × 490 HOPE Records per each hospice per year/60 minutes

per hour × \$37.02 per hour = \$1,511.65). This leads to a cost burden of \$184,792,739 across all hospices (\$32,764.67 per hospice × 5,640 hospices). Table 18 below provides the summary of changes in burden relative to the new HOPE Admission, Update Visit and Discharge timepoints. This increase in incremental burden is explained further in the Regulatory Impact Analysis (RIA) section of this proposed rule, and is also discussed in detail in the Information Collection Request accompanying this rulemaking.
BILLING CODE 4120-01-P

Table 18: Summary of Changes in Burden

Regulation Section(s)	Number of Respondents	Number of Responses (per year)	Burden per Response (hours)	Total Annual Burden (hours)	Hourly Labor Cost of Reporting (\$)	Total Cost (\$)
HOPE Admission Timepoint	5,640	2,763,850	Clinician: 0.45 Clerical: 0	Clinician: 1,243,733 Clerical: 0	Clinician at \$78.10 per hour; Clerical staff at \$37.02 per hour	\$97,135,547
HUV Timepoint	5,640	2,763,850	Clinician: 0.37 Clerical: 0.083	Clinician: 1,013,411 Clerical: 230,321	Clinician at \$78.10 per hour; Clerical staff at \$37.02 per hour	\$87,657,192
HOPE Discharge Timepoint	5,640	2,763,850	Clinician: 0 Clerical: 0	Clinician: 0 Clerical: 0	Clinician at \$78.10 per hour; Clerical staff at \$37.02 per hour	\$0
TOTAL IMPACT	5,640	2,763,850	Clinician: 0.82 Clerical: 0.083	Clinician: 2,257,144 Clerical: 230,321	Clinician at \$78.10 per hour; Clerical staff at \$37.02 per hour	\$184,792,739

BILLING CODE 4120-01-C

B. Amendment of HQRP Data Completeness Thresholds

The amended HQRP data completeness thresholds reflect the

same thresholds which have been applied to the HQRP since the FY 2018 Hospice Final Rule as they relate to HIS. As such, this proposal would not impose any additional collection of

information burden on hospices for the forthcoming Fiscal Year.

V. Response to Comments

Because of the large number of public comments we normally receive on

Federal Register documents, we are not able to acknowledge or respond to them individually. We will consider all comments we receive by the date and time specified in the **DATES** section of this preamble, and, when we proceed with a subsequent document, we will respond to the comments in the preamble to that document.

VI. Regulatory Impact Analysis

A. Statement of Need

1. Hospice Payment

This proposed rule meets the requirements of our regulations at § 418.306(c) and (d), which require annual issuance, in the **Federal Register**, of the Hospice Wage Index based on the most current available CMS hospital wage data, including any changes to the definitions of CBSAs or previously used Metropolitan Statistical Areas (MSAs), as well as any changes to the methodology for determining the per diem payment rates. This proposed rule would update the payment rates for each of the categories of hospice care, described in § 418.302(b), for FY 2025 as required under section 1814(i)(1)(C)(ii)(VII) of the Act. The payment rate updates are subject to changes in economy-wide productivity as specified in section 1886(b)(3)(B)(xi)(II) of the Act.

2. Quality Reporting Program

This proposed rule would update the requirements for HQRP to use a new standardized patient assessment tool, HOPE, which is more comprehensive than the previous HIS and includes new data elements and a new time point. These changes would allow HQRP to reflect a more consistent and holistic view of each patient's hospice election. This new reporting instrument will collect data that supports current and newly proposed quality measures included in this proposed rule and potential future quality measures. The new HOPE data elements are not only collected by chart abstraction but in real-time to adequately assess patients based on the hospice's interactions with the patient and family/caregiver, accommodate patients with varying clinical needs, and provide additional information to contribute to the patient's care plan throughout the hospice stay (not just at admission and discharge).

B. Overall Impacts

We have examined the impacts of this proposed rule as required by Executive Order 12866 on Regulatory Planning

and Review (September 30, 1993), Executive Order 14094 on Modernizing Regulatory Review (April 6, 2023), Executive Order 13563 on Improving Regulation and Regulatory Review (January 18, 2011), the Regulatory Flexibility Act (RFA) (September 19, 1980, Pub. L. 96 354), section 1102(b) of the Social Security Act, section 202 of the Unfunded Mandates Reform Act of 1995 (March 22, 1995; Pub. L. 104-4), Executive Order 13132 on Federalism (August 4, 1999), and the Congressional Review Act (CRA) (5 U.S.C. 804(2)).

Executive Orders 12866 (as amended by E.O. 14094) and E.O. 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 14094 amends 3(f) of Executive Order 12866 to define a "significant regulatory action" as an action that is likely to result in a rulemaking that: (1) has an annual effect on the economy of \$200 million or more in any 1 year, or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, territorial, or Tribal governments or communities; (2) creates a serious inconsistency or otherwise interfering with an action taken or planned by another agency; (3) materially alters the budgetary impacts of entitlement grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) raise legal or policy issues for which centralized review would meaningfully further the President's priorities or the principles set forth in this Executive Order.

A regulatory impact analysis (RIA) must be prepared for a regulatory action that is significant section 3(f)(1). Based on our estimates, OMB'S Office of Information and Regulatory Affairs has determined this rulemaking is significant under section 3(f)(1) of E.O. 12866. Accordingly, we have prepared a regulatory impact analysis presents the costs and benefits of the rulemaking to the best of our ability. Pursuant to Subtitle E of the Small Business Regulatory Enforcement Fairness Act of 1996 (also known as the Congressional Review Act), OIRA has also determined that this proposed rule meets the criteria set forth in 5 U.S.C. 804(2).

1. Hospice Payment

We estimate that the aggregate impact of the payment provisions in this

rulemaking would result in an estimated increase of \$705 million in payments to hospices, resulting from the proposed hospice payment update percentage of 2.6 percent for FY 2025. The impact analysis of this proposed rule represents the projected effects of the changes in hospice payments from FY 2024 to FY 2025. Using the most recent complete data available at the time of rulemaking, in this case FY 2023 hospice claims data as of January 11, 2024, we simulate total payments using the FY 2024 wage index (pre-floor, pre-reclassified hospital wage index with the hospice floor, and old OMB delineations with the 5-percent cap on wage index decreases) and FY 2024 payment rates and compare it to our simulation of total payments using FY 2023 utilization claims data, the proposed FY 2025 Hospice Wage Index (pre-floor, pre-reclassified hospital wage index with hospice floor, and the revised OMB delineations with a 5-percent cap on wage index decreases) and FY 2024 payment rates. By dividing payments for each level of care (RHC days 1 through 60, RHC days 61+, CHC, IRC, and GIP) using the FY 2024 wage index and payment rates for each level of care by the proposed FY 2025 wage index and FY 2024 payment rates, we obtain a wage index standardization factor for each level of care. We apply the wage index standardization factors so that the aggregate simulated payments do not increase or decrease due to changes in the wage index.

Certain events may limit the scope or accuracy of our impact analysis, because such an analysis is susceptible to forecasting errors due to other changes in the forecasted impact time period. The nature of the Medicare program is such that the changes may interact, and the complexity of the interaction of these changes could make it difficult to predict accurately the full scope of the impact upon hospices.

2. Hospice Quality Reporting Program

As proposed in section III. of this proposed rule, we are requiring implementation of a hospice patient-level item set to be used by all hospices to collect and submit standardized data on each patient admitted to hospice. Based on the cost estimates provided in the Collection of Information section above, we estimate an annual cost burden of \$184,729,739 across all hospices (\$32,764.67 per hospice × 5,640 hospices) starting in FY 2026.

BILLING CODE 4120-01-P

Table 19: Summary of Burden Hours and Costs

Regulation Section(s)	Number of Respondents	Number of Responses (per year)	Burden per Response (hours)	Total Annual Burden (hours)	Hourly Labor Cost of Reporting (\$)	Total Cost (\$)
HOPE Admission Timepoint	5,640	2,763,850	Clinician: 0.45 Clerical: 0	Clinician: 1,243,733 Clerical: 0	Clinician at \$78.10 per hour; Clerical staff at \$37.02 per hour	\$97,135,547
HUV Timepoint	5,640	2,763,850	Clinician: 0.37 Clerical: 0.083	Clinician: 1,013,411 Clerical: 230,321	Clinician at \$78.10 per hour; Clerical staff at \$37.02 per hour	\$87,657,192
HOPE Discharge Timepoint	5,640	2,763,850	Clinician: 0 Clerical: 0	Clinician: 0 Clerical: 0	Clinician at \$78.10 per hour; Clerical staff at \$37.02 per hour	\$0
TOTAL IMPACT	5,640	2,763,850	Clinician: 0.82 Clerical: 0.083	Clinician: 2,257,144 Clerical: 230,321	Clinician at \$78.10 per hour; Clerical staff at \$37.02 per hour	\$184,792,739

Our proposal would therefore result in a 2,487,466-hour annual burden (1,243,733 hours for HOPE Admissions, 1,243,733 hours for HOPE Update Visits, and 0 hours for HOPE Discharges). The total cost burden per hospice (\$32,764.67) is calculated by adding the total nursing cost with the total clerical staff cost burden. This leads to a cost burden of \$184,792,739 across all hospices (\$32,764.67 per hospice × 5,640 hospices). This burden is also discussed in detail as part of an accompanying PRA submission.

C. Detailed Economic Analysis

1. Proposed Hospice Payment Update for FY 2025

The FY 2025 proposed hospice payment impacts appear in Table 19. We tabulate the resulting payments according to the classifications (for example, provider type, geographic

region, facility size), and compare the difference between current and future payments to determine the overall impact. The first column shows the breakdown of all hospices by provider type and control (non-profit, for-profit, government, other), facility location, and facility size. The second column shows the number of hospices in each of the categories in the first column. The third column shows the effect of using the FY 2025 updated wage index data and moving from the old OMB delineations to the new revised OMB delineations with a 5-percent cap on wage index decreases. The aggregate impact of the changes in column three is zero percent, due to the hospice wage index standardization factors. However, there are distributional effects of using the FY 2025 hospice wage index. The fourth column shows the effect of the proposed hospice payment update percentage as mandated by section

1814(i)(1)(C) of the Act and is consistent for all providers. The proposed hospice payment update percentage of 2.6 percent is based on the proposed 3.0 percent inpatient hospital market basket percentage increase reduced by a proposed 0.4 percentage point productivity adjustment. The fifth column shows the total effect of the updated wage data and the hospice payment update percentage on FY 2025 hospice payments. As illustrated in Table 20, the combined effects of all the proposals vary by specific types of providers and by location. We note that simulated payments are based on utilization in FY 2023 as seen on Medicare hospice claims (accessed from the CCW on January 11, 2024) and only include payments related to the level of care and do not include payments related to the service intensity add-on.

As illustrated in Table 20, the combined effects of all the proposals

vary by specific types of providers and by location.

TABLE 20: Impact to Hospices for FY 2025

Hospice Subgroup	Hospices	FY 2025 Updated Wage Data and Revised OMB Delineations	FY 2025 Proposed Hospice Payment Update (%)	Overall Total Impact for FY 2025
All Hospices	6,044	0.0%	2.6%	2.6%
Hospice Type and Control				
Freestanding/Non-Profit	550	0.2%	2.6%	2.8%
Freestanding/For-Profit	4,012	0.0%	2.6%	2.6%
Freestanding/Government	37	-0.6%	2.6%	2.0%
Freestanding/Other	362	-0.1%	2.6%	2.5%
Facility/HHA Based/Non-Profit	316	-0.7%	2.6%	1.9%
Facility/HHA Based/For-Profit	189	0.1%	2.6%	2.7%
Facility/HHA Based/Government	71	0.2%	2.6%	2.8%
Facility/HHA Based/Other	84	-0.9%	2.6%	1.7%
Subtotal: Freestanding Facility Type	4,961	0.1%	2.6%	2.7%
Subtotal: Facility/HHA Based Facility Type	660	-0.5%	2.6%	2.1%
Subtotal: Non-Profit	866	0.0%	2.6%	2.6%
Subtotal: For Profit	4,204	0.1%	2.6%	2.7%
Subtotal: Government	108	-0.2%	2.6%	2.4%
Subtotal: Other	446	-0.2%	2.6%	2.4%
Hospice Type and Control: Rural				
Freestanding/Non-Profit	123	-0.1%	2.6%	2.5%
Freestanding/For-Profit	350	0.3%	2.6%	2.9%
Freestanding/Government	22	-0.1%	2.6%	2.5%
Freestanding/Other	55	0.5%	2.6%	3.1%
Facility/HHA Based/Non-Profit	117	0.2%	2.6%	2.8%
Facility/HHA Based/For-Profit	52	0.5%	2.6%	3.1%
Facility/HHA Based/Government	55	0.4%	2.6%	3.0%
Facility/HHA Based/Other	46	0.0%	2.6%	2.6%
Hospice Type and Control: Urban				

Freestanding/Non-Profit	427	0.2%	2.6%	2.8%
Freestanding/For-Profit	3,662	0.0%	2.6%	2.6%
Freestanding/Government	15	-0.8%	2.6%	1.8%
Freestanding/Other	307	-0.2%	2.6%	2.4%
Facility/HHA Based/Non-Profit	199	-0.9%	2.6%	1.7%
Facility/HHA Based/For-Profit	137	0.0%	2.6%	2.6%
Facility/HHA Based/Government	16	0.1%	2.6%	2.7%
Facility/HHA Based/Other	38	-1.1%	2.6%	1.5%
Hospice Location: Urban or Rural				
Rural	823	0.2%	2.6%	2.8%
Urban	5,221	0.0%	2.6%	2.6%
Hospice Location: Region of the Country (Census Division)				
New England	148	-1.4%	2.6%	1.2%
Middle Atlantic	280	-0.6%	2.6%	2.0%
South Atlantic	607	0.8%	2.6%	3.4%
East North Central	604	0.0%	2.6%	2.6%
East South Central	251	0.9%	2.6%	3.5%
West North Central	416	0.1%	2.6%	2.7%
West South Central	1,150	0.6%	2.6%	3.2%
Mountain	605	1.6%	2.6%	4.2%
Pacific	1,935	-1.8%	2.6%	0.8%
Outlying	48	-1.5%	2.6%	1.1%
Hospice Size				
0 - 3,499 RHC Days (Small)	1,600	-0.9%	2.6%	1.7%
3,500-19,999 RHC Days (Medium)	2,718	-0.2%	2.6%	2.4%
20,000+ RHC Days (Large)	1,726	0.1%	2.6%	2.7%

Source: FY 2023 hospice claims data from CCW accessed on January 11, 2024.

Note:The overall total impact reflects the addition of the individual impacts, which includes the updated wage index data and revised OMB delineations, as well as the 2.6 percent market basket update.

Due to missing Provider of Services file information (from which hospice characteristics are obtained), some subcategories in the impact tables have fewer agencies represented than the overall total (of 6,044). Subtypes involving ownership only add up to 5,624 while subtypes involving facility type only add up to 5,621.

Region Key:

New England = Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont

Middle Atlantic = Pennsylvania, New Jersey, New York

South Atlantic = Delaware, District of Columbia, Florida, Georgia, Maryland, North Carolina, South Carolina, Virginia, West Virginia

East North Central = Illinois, Indiana, Michigan, Ohio, Wisconsin

East South Central = Alabama, Kentucky, Mississippi, Tennessee

West North Central = Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota

West South Central = Arkansas, Louisiana, Oklahoma, Texas

Mountain = Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, Wyoming

Pacific = Alaska, California, Hawaii, Oregon, Washington

Outlying = Guam, Puerto Rico, Virgin Islands

2. Impacts for the Hospice Quality Reporting Program for FY 2025

The HQRP requires the active collection under OMB control number #0938–1153 (CMS 10390; expiration 01/31/2026) of the Hospice Items Set (HIS) and CAHPS® Hospice Survey (OMB control number 0938–1257 (CMS–10537; expiration 07/31/2026). Failure to submit data required under section 1814(i)(5) of the Act with respect to a CY will result in the reduction of the annual market basket percentage increase otherwise applicable to a hospice for that calendar year.

Once adopted, the Federal Government would incur costs related to the transition from HIS to HOPE. These costs would include provider training, preparation of HOPE manuals

and materials, receipt and storage of data, data analysis, and upkeep of data submission software. There are costs associated with the maintenance and upkeep of a CMS-sponsored web-based program that hospice providers would use to submit their HOPE data. In addition, the Federal Government would also incur costs for help-desk support that must be provided to assist hospices with the data submission process. There would also be costs associated with the transmission, analysis, processing, and storage of the hospice data by CMS contractors.

Also, pursuant to section 1814(i)(5)(A)(i) of the Act, hospices that do not submit the required QRP data would receive a 4 percentage point reduction of the annual market basket

increase. The Federal Government will incur additional costs associated with aggregation and analysis of the data necessary to determine provider compliance with the reporting requirements for any given fiscal year.

The total annual cost to the Federal Government for the implementation and ongoing management of HOPE data is estimated to be \$1,583,500. As this estimate is the same as the current estimated costs to the Federal Government associated with HIS, HOPE implementation and ongoing maintenance would not incur additional annual costs.

The estimated costs to hospice providers associated with HOPE are calculated as follows:

Part 1. Time Burden

Estimated Number of Admissions and Records per Hospice

	Admissions/Records	Hospices	Per Year	Per 3 Years
Admissions	2,763,850	5,640	490	1,470
Total HOPE Records	8,291,550	5,640	1,470	4,410

Estimated Number of Admissions and Records for all Hospices

	Admissions/Records	Hospices	Per 3 Years
Admissions	2,763,850	5,640	8,291,550
Total HOPE Records	8,291,550	5,640	24,874,650

Estimated HOPE Burden Hours per Year, by Time Point

Burden Hours per year (HOPE Admission)			
Discipline	Records	Hours	Total time
Clinical	2,763,850	0.45 (27 minutes)	1,243,733 hours
Clerical	2,763,850	0 (0 minutes)	0 hours
Total (HOPE Admission)			1,243,733 hours
Burden Hours per year (HOPE HUV)			
Discipline	Records	Hours	Total time
Clinical	2,763,850	0.37 (22 minutes)	1,013,411 hours
Clerical	2,763,850	0.083 (5 minutes)	230,321 hours
Total (HOPE HUV)			1,243,733 hours
Burden Hours per year (HOPE Discharge)			
Discipline	Records	Hours	Total time
Clinical	2,763,850	0 (0 minutes)	0 hours
Clerical	2,763,850	0 (0 minutes)	0 hours
Total (HOPE Discharge)			0 hours

Part 2. Cost/Wage Calculation

Note that this analysis of HOPE costs presents rounded inputs for each

calculation and based on the incremental increase of burden from the HIS timepoints. The actual calculations were performed using unrounded

inputs, so the outputs of each equation below may vary slightly from what would be expected from the rounded inputs.

Time for All Hospices

Discipline	Hours	Records	Total time
Nursing	0.82 (49 minutes)	2,763,850	2,257,144 hours
Administrative Assistant	0.08 (5 minutes)	2,763,850	230,321 hours
Total			2,487,465 hours

Table 21: Aggregate Cost Calculations

Aggregate Annual Cost Per Hospice			
Discipline	Hours	Wages	Total cost
Clinical	400.17	\$78.10	\$31,253.02
Clerical	40.83	\$37.02	\$1,511.65
Total			\$32,764.67
Aggregate Annual Cost For All Hospice Providers			
Discipline	Hours	Wages	Total cost
Clinical	2,257,144	\$78.10	\$176,282,998
Clerical	230,321	\$37.02	\$8,526,477
Total			\$184,792,739
Aggregate 3-Year Cost Per Hospice Provider			
Discipline	Hours	Wages	Total cost
Clinical	1205.4	\$78.10	\$93,760
Clerical	117.6	\$37.02	\$4,534
Total			\$98,294
Aggregate 3-Year Cost For All Hospice Providers.			
Discipline	Hours	Wages	Total cost
Clinical	6,711,432	\$78.10	\$528,848,994
Clerical	690,963	\$37.02	\$25,579,431
Total			\$554,428,425

BILLING CODE 4120-01-C

Additional details regarding these costs and calculations are available in the FY 2025 PRA package.

3. Regulatory Review Cost Estimation

If regulations impose administrative costs on private entities, such as the time needed to read and interpret this proposed rule, we should estimate the cost associated with regulatory review. Due to the uncertainty involved with accurately quantifying the number of entities that will review this rulemaking, we assume that the total number of unique commenters on last year’s proposed rule will be the number of reviewers of this proposed rule. We acknowledge that this assumption may understate or overstate the costs of reviewing this proposed rule. It is possible that not all commenters reviewed last year’s rule in detail, and it is also possible that some reviewers chose not to comment on the proposed rule. For these reasons we thought that the number of past commenters would be a fair estimate of the number of

reviewers of this proposed rule. We welcome any comments on the approach to estimating the number of entities that will review this proposed rule. We also recognize that different types of entities are in many cases affected by mutually exclusive sections of this proposed rule, and therefore for the purposes of our estimate we assume that each reviewer reads approximately 50 percent of the rulemaking. We are soliciting public comments on this assumption.

Using the occupational wage information from the BLS for medical and health service managers (Code 11–9111) from May 2022; we estimate that the cost of reviewing this rulemaking is \$100.80 per hour, including overhead and fringe benefits (<https://www.bls.gov/oes/current/oes119111.htm>). This proposed rule consists of approximately 34,385 words. Assuming an average reading speed of 250 words per minute, it would take approximately 1 hour for staff to review half of it. For each hospice that reviews the proposed rule,

the estimated cost is \$100.80 (1 hour × \$100.80). Therefore, we estimate that the total cost of reviewing this regulation is \$8,064.00 (\$100.80 × 80 reviewers).

D. Alternatives Considered

1. Hospice Payment

For the FY 2025 Hospice Wage Index and Rate Update proposed rule, we considered alternatives to the proposals articulated in section III.A of this proposed rule. We considered not proposing to adopt the OMB delineations listed in OMB Bulletin 23–01; however, we have historically adopted the latest OMB delineations in subsequent rulemaking after a new OMB Bulletin is released.

Since the hospice payment update percentage is determined based on statutory requirements, we did not consider alternatives to updating the hospice payment rates by the payment update percentage. The proposed 2.6 percent hospice payment update percentage for FY 2025 is based on a

proposed 3.0 percent inpatient hospital market basket update for FY 2025, reduced by a proposed 0.4 percentage point productivity adjustment. Payment rates since FY 2002 have been updated according to section 1814(i)(1)(C)(ii)(VII) of the Act, which states that the update to the payment rates for subsequent years must be the market basket percentage increase for that FY. Section 3401(g) of the Affordable Care Act also mandates that, starting with FY 2013 (and in subsequent years), the hospice payment update percentage will be annually reduced by changes in economy-wide productivity as specified in section 1886(b)(3)(B)(xi)(III) of the Act. For FY 2025, since the hospice payment update percentage is determined based on statutory requirements at section 1814(i)(1)(C) of the Act, we did not consider alternatives for the hospice payment update percentage.

2. Hospice Quality Reporting Program
 CMS considered proposing the HOPE instrument with more items, including data collection about the treatment and activities provided by multiple disciplines (such as medical social workers (MSW) and chaplains). However, CMS ultimately omitted those additional items, and is only proposing HOPE with items deemed relevant to current and planned quality measurement and public reporting activities.
 CMS considered proposing that hospices only need to collect HOPE data during one HUV rather than two. CMS considered changing the data submission requirement from thirty (30) days to fifteen (15) days. However, CMS determined that such a change would provide minimal benefit at this time while also being disruptive to hospice providers and this was not proposed.

E. Accounting Statement and Table
 As required by OMB Circular A-4 (available at <https://www.whitehouse.gov/wp-content/uploads/2023/11/CircularA-4.pdf>), in Table 22, we have prepared an accounting statement showing the classification of the expenditures associated with the provisions of this proposed rule. Table 22 provides our best estimate of the possible changes in Medicare payments under the hospice benefit as a result of the policies in this rulemaking. This estimate is based on the data for 6,044 hospices in our impact analysis file, which was constructed using FY 2023 claims (accessed from the CCW on January 11, 2024). All expenditures are classified as transfers to hospices. Also, Table 22 also provides the impact costs associated with the Hospice Quality Reporting Program starting FY 2026.

TABLE 22: Accounting Statement Classification of Estimated Transfers and Costs

Hospice Payment Update		FY 2024 to FY 2025	
Category		Transfers	
Annualized Monetized Transfers		\$705 million*	
From Whom to Whom?		Federal Government to Medicare Hospices	
Hospice Quality Reporting Program		FY 2026 to FY 2029	
Category		Costs	
Annualized Costs		\$185 million (2% Discount Rate)	

*The increase of \$705 million in transfer payments is a result of the 2.6 percent hospice payment update compared to payments in FY 2024.

F. Regulatory Flexibility Act (RFA)

The RFA requires agencies to analyze options for regulatory relief of small entities if a rulemaking has a significant impact on a substantial number of small entities. For purposes of the RFA, small entities include small businesses, nonprofit organizations, and small

jurisdictions. We consider all hospices as small entities as that term is used in the RFA. The North American Industry Classification System (NAICS) was adopted in 1997 and is the current standard used by the Federal statistical agencies related to the U.S. business economy. There is no NAICS code specific to hospice services. Therefore,

we utilized the NAICS U.S. industry title “Home Health Care Services” and corresponding NAICS code 621610 in determining impacts for small entities. The NAICS code 621610 has a size standard of \$19 million.³² Table 23 shows the number of firms, revenue, and estimated impact per home health care service category.

TABLE 23: NUMBER OF FIRMS, REVENUE, AND ESTIMATED IMPACT OF HOME HEALTH CARE SERVICES BY NAICS CODE 621610

NAICS Code	NAICS Description	Enterprise Size	Number of Firms	Receipts (\$1,000)	Estimated Impact (\$1,000) per Enterprise Size
621610	Home Health Care Services	<100	5,861	210,697	\$35.95
621610	Home Health Care Services	100-499	5,687	1,504,668	\$264.58
621610	Home Health Care Services	500-999	3,342	2,430,807	\$727.35
621610	Home Health Care Services	1,000-2,499	4,434	7,040,174	\$1,587.77
621610	Home Health Care Services	2,500-4,999	1,951	6,657,387	\$3,412.29
621610	Home Health Care Services	5,000-7,499	672	3,912,082	\$5,821.55
621610	Home Health Care Services	7,500-9,999	356	2,910,943	\$8,176.81
621610	Home Health Care Services	10,000-14,999	346	3,767,710	\$10,889.34
621610	Home Health Care Services	15,000-19,999	191	2,750,180	\$14,398.85
621610	Home Health Care Services	≥20,000	961	51,776,636	\$53,877.87
621610	Home Health Care Services	Total	23,801	82,961,284	\$3,485.62

Source: Data obtained from United States Census Bureau table “us_6digitnaics_rptsiz_2017” (SOURCE: 2017 County Business Patterns and Economic Census) Release Date: 5/28/2021: <https://www2.census.gov/programs-surveys/susb/tables/2017/>

Notes: Estimated impact is calculated as Receipts (\$1,000)/Number of firms.

The Department of Health and Human Services’ practice in interpreting the RFA is to consider effects economically “significant” only if greater than 5 percent of providers reach a threshold of 3 to 5 percent or more of total revenue or total costs. The majority of hospice visits are Medicare paid visits, and therefore the majority of hospice’s revenue consists of Medicare payments. Based on our analysis, we conclude that the policies proposed in this rulemaking would result in an estimated total impact of 3 to 5 percent or more on Medicare revenue for greater than 5 percent of hospices. Therefore, the Secretary has certified that this hospice proposed rule would have significant economic impact on a substantial number of small entities. We estimate that the net impact of the policies in this rule is 2.6 percent or approximately \$705 million in increased revenue to hospices in FY 2025. The 2.6 percent increase in expenditures when comparing FY 2024 payments to estimated FY 2025 payments is reflected

in the last column of the first row in Table 19 and is driven solely by the impact of the hospice payment update percentage reflected in the fifth column of the impact table. In addition, small hospices would experience a greater estimated increase (X percent), compared to large hospices (X percent) due to the proposed updated wage index. Further detail is presented in Table 19 by hospice type and location.

We estimate that the new impact of the proposed HQRP data collection requirements would be \$32,764.81 per hospice. While small hospices would be estimated to incur the same data collection impact as all other hospices, we recognize that the impact value is likely to represent a larger percentage of small provider costs. HOPE already minimizes the burden that Information Collection Requests (ICRs) place on the provider. The type of quality data specified for participation in the HQRP is already currently collected by hospices as part of their patient care processes.

In addition, section 1102(b) of the Act requires us to prepare a regulatory impact analysis if a rule may have a significant impact on the operations of a substantial number of small rural hospitals. This analysis must conform to the provisions of section 603 of the RFA. For purposes of section 1102(b) of the Act, we define a small rural hospital as a hospital that is located outside of a MSA and has fewer than 100 beds. This rulemaking would only affect hospices. Therefore, the Secretary has determined that this proposed rule would not have a significant impact on the operations of a substantial number of small rural hospitals (see Table 19).

G. Unfunded Mandates Reform Act (UMRA)

Section 202 of the Unfunded Mandates Reform Act of 1995 (UMRA) also requires that agencies assess anticipated costs and benefits before issuing any rule whose mandates require spending in any 1 year of \$100 million in 1995 dollars, updated annually for inflation. In 2024, that

³² Ibid.
 INK “https://www.sba.gov/sites/sbagov/files/2023-03/Table%20of%20Size%20Standards_

[Effective%20March%2017%2C%202023%20%281%29%20%281%29_0.pdf](https://www.sba.gov/sites/sbagov/files/2023-03/Table%20of%20Size%20Standards_Effective%20March%202017%2C%202023%20%281%29%20%281%29_0.pdf)”[https://www.sba.gov/sites/sbagov/files/2023-](https://www.sba.gov/sites/sbagov/files/2023-03/Table%20of%20Size%20Standards_Effective%20March%202017%2C%202023%20%281%29%20%281%29_0.pdf)

[03/Table%20of%20Size%20Standards_Effective%20March%202017%2C%202023%20%281%29%20%281%29_0.pdf](https://www.sba.gov/sites/sbagov/files/2023-03/Table%20of%20Size%20Standards_Effective%20March%202017%2C%202023%20%281%29%20%281%29_0.pdf)

threshold is approximately \$183 million. This rulemaking is anticipated to have an effect on State, local, or Tribal governments, in the aggregate, or on the private sector of \$183 million or more in any 1 year.

H. Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has Federalism implications. We have reviewed this rulemaking under these criteria of Executive Order 13132 and have determined that it will not impose substantial direct costs on State or local governments.

I. Conclusion

We estimate that aggregate payments to hospices in FY 2025 would increase by \$705 million as a result of the proposed hospice payment update, compared to payments in FY 2024. We estimate that in FY 2025, hospices in urban areas would experience, on average, a 2.6 percent increase in estimated payments compared to FY 2024; while hospices in rural areas would experience, on average, a 2.8 percent increase in estimated payments compared to FY 2024. Hospices providing services in the Mountain region would experience the largest estimated increases in payments of 4.2 percent. Hospices serving patients in areas in the Pacific regions would experience, on average, the lowest estimated increase of 0.8 percent in FY 2025 payments.

In accordance with the provisions of Executive Order 12866, this regulation was reviewed by the Office of Management and Budget.

Chiquita Brooks-LaSure,
Administrator of the Centers for Medicare & Medicaid Services,
approved this document on March 20, 2024.

List of Subjects in 42 CFR Part 418

Health facilities, Hospice care, Medicare, Reporting and recordkeeping requirements.

For the reasons set forth in the preamble, the Centers for Medicare & Medicaid Services proposes to amend 42 CFR chapter IV, part 418 as set forth below:

PART 418—HOSPICE CARE

■ 1. The authority citation for part 418 continues to read as follows:

Authority: 42 U.S.C. 1302 and 1395hh.

■ 2. Section 418.22 is amended by revising paragraph (c)(1)(i) to read as follows:

§ 418.22 Certification of terminal illness.

* * * * *

(c) * * *

(1) * * *

(i) The medical director of the hospice, the physician designee (as defined in § 418.3), or the physician member of the hospice interdisciplinary group; and

* * * * *

■ 3. Section 418.24 is amended by—

■ a. Revising paragraphs (a) and (b)(3);

■ b. Redesignating paragraphs (e) through (h) as paragraphs (f) through (i), respectively; and

■ c. Adding a new paragraph (e).

The revisions and addition read as follows:

§ 418.24 Election of hospice care.

(a) *Election statement.* An individual who meets the eligibility requirement of § 418.20 may file an election statement with a particular hospice. If the individual is physically or mentally incapacitated, his or her representative (as defined in § 418.3) may file the election statement.

(b) * * *

(3) Acknowledgement that the individual has been provided information on the hospice's coverage responsibility and that certain Medicare services, as set forth in paragraph (g) of this section, are waived by the election. For Hospice elections beginning on or after October 1, 2020, this would include providing the individual with information indicating that services unrelated to the terminal illness and related conditions are exceptional and unusual and hospice should be providing virtually all care needed by the individual who has elected hospice.

* * * * *

(e) *Notice of election.* The hospice chosen by the eligible individual (or his or her representative) must file the Notice of Election (NOE) with its Medicare contractor within 5 calendar days after the effective date of the election statement.

(1) *Consequences of failure to submit a timely notice of election.* When a hospice does not file the required Notice of Election for its Medicare patients within 5 calendar days after the effective date of election, Medicare will not cover and pay for days of hospice care from the effective date of election to the date of filing of the notice of election. These days are a provider liability, and the provider may not bill the beneficiary for them.

(2) *Exception to the consequences for filing the NOE late.* CMS may waive the consequences of failure to submit a timely-filed NOE specified in paragraph (e)(1) of this section. CMS will determine if a circumstance encountered by a hospice is exceptional and qualifies for waiver of the consequence specified in paragraph (e)(1) of this section. A hospice must fully document and furnish any requested documentation to CMS for a determination of exception. An exceptional circumstance may be due to, but is not limited to, the following:

(i) Fires, floods, earthquakes, or similar unusual events that inflict extensive damage to the hospice's ability to operate.

(ii) A CMS or Medicare contractor systems issue that is beyond the control of the hospice.

(iii) A newly Medicare-certified hospice that is notified of that certification after the Medicare certification date, or which is awaiting its user ID from its Medicare contractor.

(iv) Other situations determined by CMS to be beyond the control of the hospice.

■ 4. Amend § 418.25 by revising paragraph (a) and paragraph (b) introductory text to read as follows:

§ 418.25 Admission to hospice care.

(a) The hospice admits a patient only on the recommendation of the medical director (or the physician designee, as defined in § 418.3) in consultation with, or with input from, the patient's attending physician (if any).

(b) In reaching a decision to certify that the patient is terminally ill, the hospice medical director (or the physician designee, as defined in § 418.3) must consider at least the following information:

* * * * *

■ 5. Section 418.102 is amended by revising paragraph (b) introductory text and paragraph (c) to read as follows:

§ 418.102 Condition of participation: Medical director.

* * * * *

(b) *Standard: Initial certification of terminal illness.* The medical director (or physician designee, if the medical director is unavailable, as defined in § 418.3 of this section) or physician member of the IDG reviews the clinical information for each hospice patient and provides written certification that it is anticipated that the patient's life expectancy is 6 months or less if the illness runs its normal course. The physician must consider the following when making this determination:

* * * * *

(c) *Standard: Recertification of the terminal illness.* Before each recertification period for each patient, as described in § 418.21(a), the medical director (or physician designee, if the medical director is unavailable, as defined in § 418.3 of this section) or physician member of the IDG must review the patient’s clinical information.

* * * * *

§ 418.309 [Amended]

■ 6. Section 418.309 is amended in paragraphs (a)(1) and (2) by removing “2032” and adding in its place “2033”.

■ 7. Section 418.312 is amended by revising paragraph (b)(1) to read as follows:

§ 418.312 Data submission requirements under the hospice quality reporting program.

* * * * *

(b) * * *

(1) Hospices are required to complete and submit a standardized set of items for each patient to capture patient-level data, regardless of payer or patient age. The standardized set of items must be completed no less frequently than at admission, the hospice update visit (HUV), and discharge, as directed in the

associated guidance manual and required by the Hospice Quality Reporting Program. Definitions for changes in patient condition that warrant updated assessment, as well as the data elements to be completed for each applicable change in patient condition, are to be provided in sub-regulatory guidance for the current standardized hospice instrument.

* * * * *

Xavier Becerra,
Secretary, Department of Health and Human Services.

[FR Doc. 2024-06921 Filed 3-28-24; 4:15 pm]

BILLING CODE 4120-01-P



FEDERAL REGISTER

Vol. 89

Thursday,

No. 66

April 4, 2024

Part IV

Environmental Protection Agency

40 CFR Part 63

National Emission Standards for Hazardous Air Pollutants: Ethylene Production, Miscellaneous Organic Chemical Manufacturing, Organic Liquids Distribution (Non-Gasoline), and Petroleum Refineries Reconsideration; Final Action; Final Rule

**ENVIRONMENTAL PROTECTION
AGENCY**
40 CFR Part 63

[EPA-HQ-OAR-2022-0787; FRL-9846-02-OAR]

RIN 2060-AV80

**National Emission Standards for
Hazardous Air Pollutants: Ethylene
Production, Miscellaneous Organic
Chemical Manufacturing, Organic
Liquids Distribution (Non-Gasoline),
and Petroleum Refineries
Reconsideration**

AGENCY: Environmental Protection Agency (EPA).

ACTION: Final action; reconsideration of final rule.

SUMMARY: On July 6, 2020, the U.S. Environmental Protection Agency (EPA or the Agency) finalized the residual risk and technology review (RTR) conducted for the Ethylene Production source category, which is part of the Generic Maximum Achievable Control Technology Standards National Emission Standards for Hazardous Air Pollutants (NESHAP); on July 7, 2020, the EPA finalized the RTR conducted for the Organic Liquids Distribution (Non-Gasoline) NESHAP; and on August 12, 2020, the EPA finalized the RTR conducted for the Miscellaneous Organic Chemical Manufacturing NESHAP. Amendments to the Petroleum Refinery Sector NESHAP were most recently finalized on February 4, 2020. Subsequently, the EPA received and granted various petitions for reconsideration on these NESHAP for, among other things, the provisions related to the work practice standards for pressure relief devices (PRDs), emergency flaring, and degassing of floating roof storage vessels. This action finalizes proposed amendments to remove the *force majeure* exemption for PRDs and emergency flaring, incorporate clarifications for the degassing requirements for floating roof storage vessels, and address other corrections and clarifications.

DATES: This final action is effective on April 4, 2024. The incorporation by reference of certain material listed in this rule was approved by the Director of the Federal Register as of August 12, 2020.

ADDRESSES: The EPA has established a docket for this rulemaking under Docket ID No. EPA-HQ-OAR-2022-0787. All documents in the docket are listed in <https://www.regulations.gov/>. Although listed, some information is not publicly

available, *e.g.*, Confidential Business Information (CBI) or other information whose disclosure is restricted by statute. Certain other material, such as copyrighted material, is not placed on the internet and will be publicly available only in hard copy form. With the exception of such material, publicly available docket materials are available either electronically in <https://www.regulations.gov/> or in hard copy at the EPA Docket Center, WJC West Building, Room Number 3334, 1301 Constitution Avenue NW, Washington, DC. The Public Reading Room hours of operation are from 8:30 a.m. to 4:30 p.m. Eastern Standard Time (EST), Monday through Friday. The telephone number for the Public Reading Room is (202) 566-1744, and the telephone number for the EPA Docket Center is (202) 566-1742.

FOR FURTHER INFORMATION CONTACT: For questions about this final action, contact U.S. EPA, Attn: Mr. Michael Cantoni, Sector Policies and Programs Division, Mail Drop: E143-01, 109 T.W. Alexander Drive, P.O. Box 12055, RTP, North Carolina 27711; telephone number: (919) 541-5593; and email address: cantoni.michael@epa.gov.

SUPPLEMENTARY INFORMATION: *Preamble acronyms and abbreviations.* We use multiple acronyms and terms in this preamble. While this list may not be exhaustive, to ease the reading of this preamble and for reference purposes, the EPA defines the following terms and acronyms here:

atm-m³/mol atmospheres per mole per cubic meter
ACC American Chemistry Council
AFPM American Fuel and Petrochemical Manufacturers
AMEL alternative means of emissions limitation
API American Petroleum Institute
CAA Clean Air Act
CBI Confidential Business Information
CDX Central Data Exchange
CEDRI Compliance and Emissions Data Reporting Interface
CEMS continuous emission monitoring systems
CFR Code of Federal Regulations
CRA Congressional Review Act
EMACT Ethylene Production MACT
EPA Environmental Protection Agency
GMACT Generic Maximum Achievable Control Technology
HAP hazardous air pollutant(s)
ICR Information Collection Request
LEL lower explosive limit
MACT maximum achievable control technology
MCPU miscellaneous organic chemical manufacturing process unit
MON Miscellaneous Organic Chemical Manufacturing NESHAP
NAICS North American Industry Classification System

NESHAP national emission standards for hazardous air pollutants
NHV net heating value
NOCS notification of compliance status
NTTAA National Technology Transfer and Advancement Act
OLD Organic Liquids Distribution (Non-Gasoline)
OMB Office of Management and Budget
ppm parts per million
ppmv parts per million by volume
psi pounds per square inch
PRA Paperwork Reduction Act
PRD pressure relief device
RFA Regulatory Flexibility Act
RTR risk and technology review
TCEQ Texas Commission on Environmental Quality
UMRA Unfunded Mandates Reform Act

Organization of this document. The information in this preamble is organized as follows:

- I. General Information
 - A. What is the source of authority for the reconsideration action?
 - B. Does this action apply to me?
 - C. Where can I get a copy of this document and other related information?
- II. Background
 - A. Ethylene Production
 - B. Organic Liquids Distribution (Non-Gasoline)
 - C. Miscellaneous Organic Chemical Manufacturing
 - D. Petroleum Refineries
- III. Final Action
 - A. Pressure Relief Devices and Emergency Flaring
 - B. Storage Vessel Degassing
 - C. Other EMACT Standards Technical Corrections and Clarifications
 - D. Other OLD NESHAP Technical Corrections and Clarifications
 - E. Other MON Technical Corrections and Clarifications
 - F. Other Petroleum Refinery MACT 1 Technical Corrections and Clarifications
 - G. What compliance dates are we finalizing?
- IV. Summary of Cost, Environmental, and Economic Impacts
 - A. What are the affected facilities?
 - B. What are the air quality impacts?
 - C. What are the cost impacts?
 - D. What are the economic impacts?
 - E. What are the benefits?
 - F. What analysis of environmental justice did we conduct?
- V. Statutory and Executive Order Reviews
 - A. Executive Order 12866: Regulatory Planning and Review and Executive Order 14094: Modernizing Regulatory Review
 - B. Paperwork Reduction Act (PRA)
 - C. Regulatory Flexibility Act (RFA)
 - D. Unfunded Mandates Reform Act (UMRA)
 - E. Executive Order 13132: Federalism
 - F. Executive Order 13175: Consultation and Coordination With Indian Tribal Governments
 - G. Executive Order 13045: Protection of Children From Environmental Health Risks and Safety Risks
 - H. Executive Order 13211: Actions Concerning Regulations That

- Significantly Affect Energy Supply, Distribution, or Use
- I. National Technology Transfer and Advancement Act (NTTAA) and 1 CFR Part 51
- J. Executive Order 12898: Federal Actions To Address Environmental Justice in Minority Populations and Low-Income Populations and Executive Order 14096: Revitalizing Our Nation's Commitment to Environmental Justice for All
- K. Congressional Review Act (CRA)

I. General Information

A. What is the source of authority for the reconsideration action?

The statutory authority for this action is provided by sections 112 and

307(d)(7)(B) of the Clean Air Act (CAA) (42 U.S.C. 7412 and 7607(d)(7)(B)).

B. Does this action apply to me?

Table 1 of this preamble lists the NESHAP and associated regulated industrial source categories that are the subject of this action. Table 1 is not intended to be exhaustive, but rather provides a guide for readers regarding the entities that this action is likely to affect. The final standards will be directly applicable to the affected sources. Federal, State, local, and Tribal government entities are not affected by this action. Each of the source categories covered by this action were defined in

the *Initial List of Categories of Sources Under Section 112(c)(1) of the Clean Air Act Amendments of 1990* (see 57 FR 31576; July 16, 1992) and *Documentation for Developing the Initial Source Category List, Final Report* (see EPA-450/3-91-030, July 1992), as well as the *National Emission Standards for Hazardous Air Pollutants; Revision of Initial List of Categories of Sources and Schedule for Standards Under Sections 112(c) and (e) of the Clean Air Act Amendments of 1990* (61 FR 28197; June 4, 1996), as presented here.

TABLE 1—NESHAP AND INDUSTRIAL SOURCE CATEGORIES AFFECTED BY THIS FINAL ACTION

Source category	NESHAP	NAICS ¹ code
Ethylene Production	40 CFR part 63, subparts XX and YY	325110.
Organic Liquids Distribution (Non-Gasoline)	40 CFR part 63, subpart EEEE	3222, 3241, 3251, 3252, 3259, 3261, 3361, 3362, 3399, 4247, 4861, 4869, 4931, 5622.
Miscellaneous Organic Chemical Manufacturing.	40 CFR part 63, subpart FFFF	3251, 3252, 3253, 3254, 3255, 3256, and 3259, with several exceptions.
Petroleum Refineries	40 CFR part 63, subpart CC	324110.

¹ North American Industry Classification System (NAICS).

The Ethylene Production source category includes any chemical manufacturing process unit in which ethylene and/or propylene are produced by separation from petroleum refining process streams or by subjecting hydrocarbons to high temperatures in the presence of steam. The ethylene production unit includes the separation of ethylene and/or propylene from associated streams such as a C₄ product,¹ pyrolysis gasoline, and pyrolysis fuel oil. The ethylene production unit does not include the manufacture of Synthetic Organic Chemical Manufacturing Industry (SOCMI) chemicals such as the production of butadiene from the C₄ stream and aromatics from pyrolysis gasoline.

The Organic Liquids Distribution (Non-Gasoline) source category includes, but is not limited to, those activities associated with the storage and distribution of organic liquids other than gasoline, at sites which serve as distribution points from which organic liquids may be obtained for further use and processing. The distribution activities include the storage of organic liquids in storage tanks not subject to other 40 CFR part 63 standards and transfers into or out of the tanks from or

to cargo tanks, containers, and pipelines.

Following the initial source category listings, the Agency combined 21 of the 174 originally defined source categories, and other organic chemical processes which were not included in the original 174 source category list, into one source category called the “Miscellaneous Organic Chemical Processes” source category.² The Agency later divided the “Miscellaneous Organic Chemical Processes” source category into two new source categories called the “Miscellaneous Organic Chemical Manufacturing” source category and the “Miscellaneous Coating Manufacturing” source category.³ The Miscellaneous Organic Chemical Manufacturing source category includes any facility engaged in the production of benzyltrimethylammonium chloride, carbonyl sulfide chelating agents, chlorinated paraffins, ethylidene norbornene, explosives, hydrazine, photographic chemicals, phthalate plasticizers, rubber chemicals, symmetrical tetrachloropyridine, oxybisphenoxarsine/1,3-diisocyanate, alkyd resins, polyester resins, polyvinyl alcohol, polyvinyl acetate emulsions, polyvinyl butyral, polymerized vinylidene chloride, polymethyl methacrylate, maleic anhydride copolymers, or any other organic

chemical processes not covered by another maximum available control technology (MACT) standard. Many of these organic chemical processes involve similar process equipment, similar emission points and control equipment, and are in many cases co-located with other source categories.

The Petroleum Refineries sector includes two source categories. The Petroleum Refineries MACT 1 source category includes any facility engaged in producing gasoline, naphthas, kerosene, jet fuels, distillate fuel oils, residual fuel oils, lubricants, or other products from crude oil or unfinished petroleum derivatives. The refinery process units in this source category include, but are not limited to, thermal cracking, vacuum distillation, crude distillation, hydroheating/hydrorefining, isomerization, polymerization, lube oil processing, and hydrogen production. The Petroleum Refineries MACT 2—Catalytic Cracking (Fluid and Other) Units, Catalytic Reforming Units, and Sulfur Recovery Units source category includes any facility engaged in producing gasoline, naphthas, kerosene, jet fuels, distillate fuel oils, residual fuel oils, lubricants, or other products from crude oil or unfinished petroleum derivatives.

¹ The C₄ product stream is a hydrocarbon product stream from an ethylene production unit consisting of compounds with four carbon atoms (*i.e.*, butanes, butenes, butadienes).

² 61 FR 57602 (Nov. 7, 1996).

³ 64 FR 63035 (Nov. 18, 1999).

C. Where can I get a copy of this document and other related information?

In addition to being available in the docket, an electronic copy of this final action will also be available on the internet. Following signature by the EPA Administrator, the EPA will post a copy of this final action at <https://www.epa.gov/stationary-sources-air-pollution/petroleum-refinery-sector-rule-risk-and-technology-review-and-new>, <https://www.epa.gov/stationary-sources-air-pollution/acetal-resins-acrylic-modacrylic-fibers-carbon-black-hydrogen>, <https://www.epa.gov/stationary-sources-air-pollution/miscellaneous-organic-chemical-manufacturing-national-emission>, and <https://www.epa.gov/stationary-sources-air-pollution/organic-liquids-distribution-national-emission-standards-hazardous>. Following publication in the **Federal Register**, the EPA will post the **Federal Register** version and key technical documents at these same websites.

Copies of all comments received on the proposed rulemaking (National Emission Standards for Hazardous Air Pollutants: Ethylene Production, Miscellaneous Organic Chemical Manufacturing, Organic Liquids Distribution (Non-Gasoline), and Petroleum Refineries Reconsideration)⁴ are available at the EPA Docket Center Public Reading Room. Comments are also available electronically through <https://www.regulations.gov/> by searching Docket ID No. EPA-HQ-OAR-2022-0787.

Redline strikeout versions of each rule showing the edits that incorporate the changes finalized in this action are presented in the documents titled: *Final Regulatory Text Edits for Subpart EEEE*, *Final Regulatory Text Edits for Subpart FFFF*, *Final Regulatory Text Edits for Subpart YY*, and *Final Regulatory Text Edits for Subpart CC*, available in the docket for this action (Docket ID No. EPA-HQ-OAR-2022-0787).

II. Background

Following the EPA's finalization of the risk and technology reviews for the Ethylene Production (or EMACT), Organic Liquids Distribution (Non-Gasoline) (OLD), and Miscellaneous Organic Chemical Manufacturing (MON) NESHAP in 2020, the EPA also received petitions for reconsideration of these actions. The EPA also received a petition for reconsideration of the Petroleum Refinery Sector NESHAP raising some of the same issues.

To address selected issues for which we granted reconsideration and to provide other technical corrections, the EPA is finalizing revisions to the EMACT standards, OLD NESHAP, MON, and Petroleum Refineries NESHAP. The EPA is finalizing revisions to the work practice standards for PRDs and emergency flaring related to *force majeure* provisions in the EMACT standards, MON, and Petroleum Refineries NESHAP, and is finalizing standards for the degassing of storage vessels in the EMACT standards, OLD NESHAP, and MON. The EPA is also adding requirements for pressure-assisted flares and mass spectrometers to the Petroleum Refineries NESHAP to align this rule with other more recent chemical sector rules and eliminate the need to request site-specific alternative means of emission limitations (AMELs) for these units. In addition, the EPA is finalizing other technical corrections, clarifications, and correction of typographical errors in all rules. As explained in the proposed rule, the EPA requested comment only on specific issues identified in the document and explained that it would not address other issues or provisions of these final rules not specifically address in the proposed rule.

A. Ethylene Production

The MACT standards for the Ethylene Production source category (herein called the EMACT standards) are contained in the Generic Maximum Achievable Control Technology (GMACT) NESHAP, which also includes MACT standards for several other source categories. The EMACT standards were promulgated on July 12, 2002,⁵ and codified at 40 CFR part 63, subparts XX and YY. As promulgated in 2002, and further amended,⁶ the EMACT standards regulate hazardous air pollutant (HAP) emissions from ethylene production units located at major sources. An ethylene production unit is a chemical manufacturing process unit in which ethylene and/or propylene are produced by separation from petroleum refining process streams or by subjecting hydrocarbons to high temperatures in the presence of steam. The EMACT standards define the affected source as all storage vessels, ethylene process vents, transfer racks, equipment, waste streams, heat exchange systems, and ethylene cracking furnaces and associated decoking operations that are associated with each ethylene production unit

located at a major source as defined in CAA section 112(a)(1).

Following promulgation of the EMACT standards in July 2020, the EPA received two petitions for reconsideration in September 2020. The EPA received a joint petition from the American Chemistry Council (ACC) and the American Fuel & Petrochemical Manufacturers (AFPM). The EPA also received a petition from Earthjustice (on behalf of RISE St. James, Louisiana Bucket Brigade, Louisiana Environmental Action Network, Texas Environmental Justice Advocacy Services, Air Alliance Houston, Community In-Power & Development Association, Clean Air Council, Center for Biological Diversity, Environmental Integrity Project, and Sierra Club). Copies of the petitions are provided in the docket for this action (see Docket Item No. EPA-HQ-OAR-2022-0787-0005 and EPA-HQ-OAR-2022-0787-0006). ACC/AFPM's petition requested that the EPA reconsider certain aspects of the final action including, among other things, the storage vessel degassing provisions, ethylene cracking furnace burner repair provisions, and ethylene cracking furnace isolation valve inspections. Earthjustice's petition requested that the EPA reconsider certain aspects of the final rule including, among other things, the *force majeure* and exemption allowances in the work practice standards for PRDs and emergency flaring. ACC/AFPM and Earthjustice also raised other issues that are not addressed in this rulemaking.

On April 19, 2022, the EPA informed the petitioners, ACC/AFPM, and Earthjustice that it would grant reconsideration of the provisions addressing the work practice standards for PRDs, emergency flaring, and degassing of floating roof storage vessels, under CAA section 307(d)(7)(B). The EPA also informed the petitioners of the continuing review of all issues raised in their petitions. A copy of the letter to the petitioners is available in the docket for this action (see Docket Item No. EPA-HQ-OAR-2022-0787-0022).

The EPA proposed the reconsideration of the EMACT standards to address these issues along with other technical corrections and clarifications and requested public comment.⁷

With the exception of out-of-scope comments, this final preamble provides summaries and responses to all comments received regarding the proposed reconsideration of the EMACT standards. Comments on the proposed

⁵ 67 FR 46258 (Jul. 12, 2002).

⁶ 70 FR 19266 (Apr. 13, 2005); 85 FR 40386 (Jul. 6, 2020).

⁷ 88 FR 25574 (Apr. 27, 2023).

⁴ 88 FR 25574 (Apr. 27, 2023).

reconsideration of the EMACT standards that we consider out of scope for this reconsideration rulemaking include comments on the standards for PRDs and emergency flaring that discuss topics other than the *force majeure* provisions.

B. Organic Liquids Distribution (Non-Gasoline)

The Organic Liquids Distribution (Non-Gasoline) (herein called OLD NESHAP) is codified at 40 CFR part 63, subpart EEEE.⁸ Organic liquids are any crude oils downstream of the first point of custody transfer and any non-crude oil liquid that contains at least 5 percent by weight of any combination of the 98 HAP listed in table 1 of 40 CFR part 63, subpart EEEE. For the purposes of the OLD NESHAP, as promulgated in 2004, and further amended,⁹ organic liquids do not include gasoline, kerosene (No. 1 distillate oil), diesel (No. 2 distillate oil), asphalt, and heavier distillate oil and fuel oil, fuel that is consumed or dispensed on the plant site, hazardous waste, wastewater, ballast water, or any non-crude liquid with an annual average true vapor pressure less than 0.7 kilopascals (0.1 pounds per square inch (psi)). Emission sources controlled by the OLD NESHAP are storage tanks, transfer operations, transport vehicles while being loaded, and equipment leak components (valves, pumps, and sampling connections) that have the potential to leak at major sources.

The EPA received three petitions for reconsideration for the OLD NESHAP in September 2020. The EPA received petitions from Stoel Rives LLP (on behalf of Alyeska Pipeline Company), the American Petroleum Institute (API) and AFPM, and Earthjustice (on behalf of California Communities Against Toxics, Coalition for a Safe Environment, and Sierra Club). Copies of the petitions are provided in the docket for this rulemaking (see Docket Item No. EPA-HQ-OAR-2022-0787-0015, EPA-HQ-OAR-2022-0787-0023, and EPA-HQ-OAR-2022-0787-0004). API/AFPM and Stoel Rives LLP (on behalf of Alyeska Pipeline Company) requested that the EPA reconsider its final action and specifically raised the issue of storage vessel degassing. In their respective petitions, API/AFPM, Stoel Rives, and Earthjustice also raised other issues that are not being addressed in this rulemaking.

On September 8, 2021, the EPA informed petitioners Stoel Rives, API/

AFPM, and Earthjustice that it would grant reconsideration on certain issues, including the work practice standards for storage vessel degassing that apply broadly, under CAA section 307(d)(7)(B). Other issues for which EPA granted voluntary reconsideration in the September 8, 2021, letter (*e.g.*, work practice standards for venting from conservation vents on the Valdez Marine Terminal's crude oil fixed roof tanks and fence-line monitoring) are still being reviewed and are not part of this action. The EPA also stated in the letter to the petitioners that it is continuing to review all issues raised in the petitions. A copy of the letter to petitioners is available in the docket for this action (see Docket Item No. EPA-HQ-OAR-2022-0787-0016).

On April 27, 2023, the EPA proposed to reconsider, and requested comment on, the OLD NESHAP to address storage vessel degassing along with other technical corrections and clarifications.¹⁰

With the exception of out-of-scope comments, this final preamble provides summaries and responses to all comments received regarding the proposed reconsideration of the OLD NESHAP. Comments on the proposed reconsideration of the OLD NESHAP that we consider out of scope for this reconsideration rulemaking include comments on the standards for PRDs and emergency flaring that discuss topics other than the *force majeure* provisions and comments on requirements for temporary control devices.

C. Miscellaneous Organic Chemical Manufacturing

The NESHAP for the Miscellaneous Organic Chemical Manufacturing source category (herein called MON) is codified at 40 CFR part 63, subpart FFFF.¹¹ As promulgated in 2003, and further amended,¹² the MON regulates HAP emissions from miscellaneous organic chemical manufacturing process units (MCPUs) located at major sources. A miscellaneous organic chemical manufacturing process unit (MCPU) includes a miscellaneous organic chemical manufacturing process, as defined in 40 CFR 63.2550(i), and must meet the following criteria: it manufactures any material or family of materials described in 40 CFR 63.2435(b)(1); it processes, uses, or generates any of the organic HAP described in 40 CFR 63.2435(b)(2); and,

except for certain process vents that are part of a chemical manufacturing process unit, as identified in 40 CFR 63.100(j)(4), the MCPU is not an affected source or part of an affected source under another subpart of 40 CFR part 63. An MCPU also includes any assigned storage tanks and transfer racks; equipment in open systems that is used to convey or store water having the same concentration and flow characteristics as wastewater; and components such as pumps, compressors, agitators, PRDs, sampling connection systems, open-ended valves or lines, valves, connectors, and instrumentation systems that are used to manufacture any material or family of materials described in 40 CFR 63.2435(b)(1). Sources of HAP emissions regulated by the MON include the following: process vents, storage tanks, transfer racks, equipment leaks, wastewater streams, and heat exchange systems.

Following promulgation of the MON in August 2020, the EPA received five petitions for reconsideration between October and December 2020. The EPA received petitions from the ACC (who submitted two petitions), the Texas Commission on Environmental Quality (TCEQ), Huntsman Petrochemical, LLC, and Earthjustice (on behalf of RISE St. James, Louisiana Bucket Brigade, Louisiana Environmental Action Network, Texas Environmental Justice Advocacy Services, Air Alliance Houston, Ohio Valley Environmental Coalition, Blue Ridge Environmental Defense League, Environmental Justice Health Alliance for Chemical Policy Reform, Sierra Club, Environmental Integrity Project, and Union of Concerned Scientists). Copies of the petitions are provided in the docket for this rulemaking (see Docket Item Nos. EPA-HQ-OAR-2022-0787-0007, EPA-HQ-OAR-2022-0787-0009, EPA-HQ-OAR-2022-0787-0010, EPA-HQ-OAR-2022-0787-0027, and EPA-HQ-OAR-2022-0787-0008). ACC's petitions requested that the EPA reconsider certain aspects of the final rule including, among other things, the storage vessel degassing provisions and requirements for ethylene oxide sources. Earthjustice's petition requested that the EPA reconsider certain aspects of the final rule including, among other things, the *force majeure* and exemption allowances for PRDs and emergency flaring. TCEQ, ACC, and Huntsman Petrochemical's petitions requested that the EPA reassess the MON risk assessment for issues around ethylene oxide risks. The EPA addressed ACC, TCEQ, and Huntsman Petrochemical's

⁸ 69 FR 5038 (Feb. 3, 2004).

⁹ 71 FR 42898 (Jul. 28, 2006); 73 FR 21825 (Apr. 23, 2008); 73 FR 40977 (Jul. 17, 2008), and 85 FR 40740 (Jul. 7, 2020).

¹⁰ 88 FR 25574 (Apr. 27, 2023).

¹¹ 68 FR 63852 (Nov. 10, 2003).

¹² 70 FR 38562 (July 1, 2005); 71 FR 40316 (Jul. 14, 2006); and 85 FR 49084 (Aug. 12, 2020).

reconsideration petitions in a separate rulemaking.¹³ Earthjustice and ACC also raised other issues that are not being addressed in this rulemaking.

On June 17, 2021, the EPA sent a letter to petitioners informing them that it is continuing to review all issues raised in the petitions. A copy of the letter to petitioners is available in the docket for this action (see Docket Item No. EPA-HQ-OAR-2022-0787-0017).

On April 27, 2023, the EPA proposed the reconsideration of the MON to address these issues along with other technical corrections and clarifications and requested public comment.¹⁴

With the exception of out-of-scope comments, this final preamble provides summaries and responses to all comments received regarding the proposed reconsideration of the MON. Comments on the proposed reconsideration of the MON that we consider out of scope for this reconsideration rulemaking include:

- Comments on the standards for PRDs and emergency flaring that discuss topics other than the *force majeure* provisions, including releases from PRDs in ethylene oxide service and PRD monitoring.
- Comments on surge control vessel or bottoms receiver vents.
- Comments on maintenance vent provisions.
- Comments on conservation vent provisions.

D. Petroleum Refineries

The EPA finalized amendments to the petroleum refinery sector rules as the result of an RTR.¹⁵ These amendments included, among other provisions, adding work practice requirements to Petroleum Refinery MACT 1 (40 CFR part 63, subpart CC) for PRDs and flares in 40 CFR 63.648(j) and 63.670(o), respectively. These provisions specifically provide requirements for owners and operators to follow in the event of an atmospheric PRD release or emergency flaring event including performing root cause analysis for each event and implementing corrective action(s) in accordance with the rule requirements.

The EPA received three petitions to reconsider the December 2015 final rule. Two petitions were filed on January 19, 2016, and February 1, 2016, jointly by API and the AFPM. In response to API/AFPM's January 19, 2016, petition for reconsideration, the EPA issued a proposal on February 9, 2016,¹⁶ and a

final rule on July 13, 2016.¹⁷ The third petition was filed on February 1, 2016, by Earthjustice on behalf of Air Alliance Houston, California Communities Against Toxics, the Clean Air Council, the Coalition for a Safe Environment, the Community In-Power & Development Association, the Del Amo Action Committee, the Environmental Integrity Project, the Louisiana Bucket Brigade, the Sierra Club, the Texas Environmental Justice Advocacy Services, and Utah Physicians for a Healthy Environment. In their petition, Earthjustice claimed that several aspects of the revisions to the Petroleum Refinery MACT 1 were not proposed; therefore, the public was precluded from commenting on the altered provisions during the public comment period, including, among other provisions, the work practice standard for PRDs and emergency flaring.

On June 16, 2016, the EPA informed petitioners it would grant reconsideration on issues where petitioners claimed they had not been provided an opportunity to comment. Subsequently, the EPA proposed the reconsideration of the Petroleum Refinery MACT 1 to address issues for which reconsideration was granted in the June 16, 2016, letters.¹⁸ The EPA solicited public comment on five issues in the proposal related to the work practice standard for PRDs, the work practice standard for emergency flaring events, and the assessment of risk as modified based on implementation of these PRD and emergency flaring work practice standards. On February 4, 2020, the EPA issued a final action¹⁹ setting forth its decisions on each of the five issues.

On April 6, 2020, Earthjustice submitted a petition for reconsideration of the February 2020 final action on behalf of Air Alliance Houston, California Communities Against Toxics, Clean Air Council, Coalition For A Safe Environment, Community In-Power & Development Association, Del Amo Action Committee, Environmental Integrity Project, Louisiana Bucket Brigade, Sierra Club, Texas Environmental Justice Advocacy Services, and Utah Physicians for a Healthy Environment (see Docket Item No. EPA-HQ-OAR-2022-0787-0029). The petition for reconsideration requested that the EPA reconsider five issues in the February 4, 2020, final rule: (1) The EPA's rationale that the PRD standards and emergency flaring standards are continuous; (2) the EPA's

rationale for the PRD standards under CAA sections 112(d)(2) and (3); (3) the EPA's rationale for separate work practice standards for flares operating above the smokeless capacity; (4) the EPA's rationale for risk acceptability and risk determination; and (5) the EPA's analysis and rationale in its assessment of acute risk. The EPA initially denied the April 6, 2020, petition for reconsideration²⁰ and provided detailed responses to each of the five issues raised in the April 2020 petition in a September 3, 2020, letter, which is available in the Petroleum Refinery rulemaking docket (see Docket Item No. EPA-HQ-OAR-2010-0682-0999). After further consideration, on April 19, 2022, EPA informed petitioners that it would undertake reconsideration on select provisions related to the work practice standard for PRDs and emergency flaring (see Docket Item No. EPA-HQ-OAR-2022-0787-0003). Specifically, the EPA is reconsidering the inclusion of the *force majeure* allowances in the PRD and emergency flaring work practice standard. As noted in our April 19, 2022, letter, we may reconsider additional issues in the future.

On April 27, 2023, the EPA proposed the reconsideration of Petroleum Refinery MACT 1 to address the PRD and emergency flaring work practice standard along with other technical corrections and clarifications and requested public comment.²¹

With the exception of out-of-scope comments, this final preamble provides summaries and responses to all comments received regarding the proposed reconsideration of the Petroleum Refinery MACT 1. Comments on the proposed reconsideration of the Petroleum Refinery MACT 1 that we consider out of scope for this reconsideration rulemaking include comments on the standards for PRDs and emergency flaring that discuss topics other than the *force majeure* provisions.

III. Final Action

In this section of the preamble, the EPA sets forth its final decisions on the issues for which reconsideration was granted and on which the EPA solicited comment in the April 27, 2023, proposed rule.²² We also present the Agency's rationale for the decisions. The EPA is finalizing revisions to the work practice standards for PRDs and emergency flaring related to *force majeure* provisions in the EMACT

¹³ 87 FR 77985 (Dec. 21, 2022).

¹⁴ 88 FR 25574 (Apr. 27, 2023).

¹⁵ 80 FR 75178 (Dec. 1, 2015).

¹⁶ 81 FR 6814 (Feb. 9, 2016).

¹⁷ 81 FR 45232 (Jul. 13, 2016).

¹⁸ 81 FR 71661 (Oct. 18, 2016).

¹⁹ 85 FR 6064 (Feb. 4, 2020).

²⁰ 85 FR 67665 (April 6, 2020).

²¹ 88 FR 25574 (Apr. 27, 2023).

²² 88 FR 25574 (Apr. 27, 2023).

standards, MON, and Petroleum Refinery MACT 1 and is also finalizing clarifications for the degassing of storage vessels in the EMACT standards, OLD NESHAP, and MON. In addition, the EPA is finalizing requirements for pressure-assisted flares and mass spectrometers in the Petroleum Refinery MACT 1 to align this rule with other more recent chemical sector rules and to eliminate the need to request site specific alternative means of emission limitations (AMELs) for these units. Also, the EPA is finalizing other technical corrections, clarifications, and correction of typographical errors in all rules. The sections below provide a brief summary of each topic as well as summaries and responses to the comments received on each topic.

A. Pressure Relief Devices and Emergency Flaring

Topic summary: Petroleum Refinery MACT 1, EMACT standards, and the MON include work practice standards for PRDs and emergency flaring. These provisions specifically provide requirements for owners and operators to follow in the event of an atmospheric PRD release or emergency flaring event including performing root cause analysis for each event and implementing corrective action(s) in accordance with the rule requirements. The atmospheric PRD release and emergency flaring provisions specify the conditions which result in a violation of the work practice standards. The owner or operator is required to track the number of events by emission unit and root cause. An atmospheric PRD release or emergency flaring event for which the root cause is determined to be poor maintenance or operator error is a violation of the WPS. Two atmospheric PRD releases or two emergency flaring events from the same emission unit which are determined to be the result of the same root cause in a 3-year period is a violation of the work practice standard. Finally, three atmospheric PRD releases or three emergency flaring events from the same emission unit regardless of the root cause is a violation of the work practice standard (also referred to as “the ‘three strikes’ provisions”). Notably, if the root cause is determined to be due to a *force majeure* event, as defined in 40 CFR 63.641, 40 CFR 63.1103(e)(2), and 40 CFR 63.2550, it does not count towards the criteria for a violation of the WPS. However, in reconsidering these provisions, the EPA has recognized that despite the term *force majeure* being carefully defined, the *force majeure* allowance in the work practice standards may present difficulties for

determining compliance. It may also represent a provision that some facility owners or operators may seek to use to avoid incurring violations and pursuing potentially disruptive corrective actions. During the root cause analysis and corrective action process, owners or operators maintain discretion when categorizing and reporting the root cause of atmospheric PRD releases and emergency flaring events, thereby placing the onus on the EPA to determine whether the definition of *force majeure* was appropriately applied.

In light of these concerns, we reviewed periodic reports from refineries in Texas and Louisiana obtained through the EPA Regional Office (Docket ID No. EPA-HQ-OAR-2022-0787-0021 and EPA-HQ-OAR-2022-0787-0025). Based on the data available, we concluded that the frequency of these types of releases is lower than originally expected. We also found that by removing the *force majeure* allowance, the rule is strengthened, and compliance becomes easier to assess as it is determined purely based on the count of events by emission unit and root cause. As such, the EPA proposed to remove the *force majeure* provisions from the PRD and emergency flaring work practice standards. See section III.A. of the preamble to the proposed rule for additional details.²³

Comments: A commenter supported the proposed decision to remove *force majeure* provisions from the PRD and emergency flaring work practice standards. The commenter stated that the EPA’s evaluation of refinery periodic reports appropriately concluded the provisions are not needed and that compliance with the provisions would become easier for facilities and for the EPA to evaluate. The commenter further stated the *force majeure* provisions should be removed because they are unlawful and mean that an emission standard does not apply at all times for PRDs and flaring. The commenter contended that to ensure that standards apply at all times for PRDs, the EPA must specify that any uncontrolled release from a PRD is a violation of the standard. For a standard to apply at all times for flaring, the commenter asserted that the EPA has not shown how a flare will comply with the net heating value of the combustion zone limit and achieve 98 percent destruction while smoking.

Other commenters opposed the proposed decision to remove *force majeure* provisions from the PRD and

emergency flaring work practice standards. Some of these commenters argued that the EPA evaluated too narrow of a dataset to identify *force majeure* events. They stated that evaluating data over a longer period is necessary, due to the infrequent nature of *force majeure* events. They also emphasized that the review was not representative of all affected source categories, because only data from petroleum refineries were analyzed. Furthermore, one commenter contended that considering the frequency of events was not an adequate basis for removing the provisions.

Some commenters stated it was not appropriate to remove the *force majeure* provisions because these events are beyond the control of a facility and a facility should not be held liable for PRD releases or smoking flares during these events. A commenter argued that considering the difficulty of enforcing the standard is not a rational basis to remove *force majeure* provisions. The commenter also noted the fact that few *force majeure* events were identified indicates that facilities are not abusing the provisions. A commenter stated that removing the *force majeure* provisions could create resource burdens for local authorities if there is an increase in violations.

Response: After consideration of the comments submitted, the EPA is finalizing the revisions as proposed and removing the *force majeure* allowance from the criteria for a violation of the work practice standards for atmospheric PRD releases and emergency flaring events. Commenters indicated that the basis for the EPA’s conclusion that the *force majeure* exemption was rarely used was because it only took into consideration three years of data. However, this 3-year period is the period for which the work practice standards were in effect for refineries and thus we believe that this is the best available data from which to draw conclusions on the efficacy and necessity of the elements of the work practice standards (Standards under CAA section 112 are to reflect emissions limitations “for which the Administrator has emissions information.”). Although some commenters indicate that there were major weather events that could have caused relief events from PRDs or flare smoking events, they did not provide any detailed information on whether any PRD or flare smoking events actually occurred from these weather events.

In addition, as the EPA has consistently explained, in the event that a source fails to comply with the

²³ 88 FR 25580 (Apr. 27, 2023).

applicable CAA section 112 standards, the EPA would determine an appropriate response based on, among other things, the good faith efforts of the source to minimize emissions during the violative periods, including preventative and corrective actions, as well as root cause analyses to ascertain and rectify excess emissions. Thus, while this action removes the *force majeure* provisions from the PRD and emergency flaring work practice standards, the EPA will continue to evaluate violations on a case-by-case basis and determine whether an enforcement action is appropriate. If the EPA determines in a particular case that enforcement action against a source for violation of a standard is warranted, the source can raise any and all defenses in that enforcement action and the federal district court will determine what, if any, relief is appropriate. The same is true for citizen enforcement actions.

Regarding the comment that the work practice standards do not provide continuous standards, we disagree with this comment. We have previously addressed this issue and the EPA's position that the *force majeure* provisions do not make the standards non-continuous has not changed. We addressed this in the preamble to the proposed rule²⁴ where we explained that we had previously addressed this in a September 2020 letter to Earthjustice (Docket Item No. EPA-HQ-OAR-2010-0682-0999). Components of both the PRD management provisions and emergency flaring provisions apply at all times; not all components of the standard must apply at all times for the standard to be continuous.

Therefore, in this final action for Petroleum Refinery MACT 1, the EPA is removing the *force majeure* allowance from the criteria for a violation of the work practice standard for atmospheric PRD releases and emergency flaring events in 40 CFR 63.648(j)(3) and 63.670(o)(7). We are also amending the reporting requirements for the event-specific work practice standard data in 40 CFR 63.655(g)(10)(iv) and (11)(iv) to require these data to be reported electronically through the EPA's Central Data Exchange (CDX) using the Compliance and Emissions Data Reporting Interface (CEDRI). As further discussed in section III.G. of this preamble, we are finalizing that the removal of the *force majeure* provisions is effective 60 days after the effective date of the final rule.

For flares, the EMACT standards and MON cross reference the petroleum refinery flare provisions at 40 CFR

63.670. Therefore, the revisions to 40 CFR 63.670(o)(7) for emergency flaring events are incorporated into the requirements for these regulations.

The EPA is also revising the EMACT standards and the MON consistent with our proposal. We are removing the *force majeure* allowance from the criteria for a violation of the work practice standard for atmospheric PRD releases in 40 CFR 63.1107(h)(3) and 63.2480(e)(3) going forward. However, we are not removing the term *force majeure* from the list of defined terms in 40 CFR 63.1103(e)(2) and 63.2550. As further discussed in section III.G. of this preamble, we are finalizing that the removal of the *force majeure* provisions is effective 60 days after the effective date of the final rule. Lastly, the EPA is finalizing new reporting requirements for the EMACT standards at 40 CFR 63.1110(a)(10)(iii) to require electronic reporting, through the CDX using CEDRI, of the event-specific work practice standard data in 40 CFR 63.1110(e)(4)(iv) and 63.1110(e)(8)(iii). We note that the MON already has a more general compliance report template for electronic reporting, see 40 CFR 63.2520(e), which will automatically incorporate electronic reporting of the event-specific work practice standard data.

B. Storage Vessel Degassing

Topic summary: The EMACT standards, OLD NESHAP, and MON currently include a work practice standard for storage vessel degassing to control emissions from shutdown operations (see 40 CFR 63.1103(e)(10), 40 CFR 63.2346(a)(6), and 40 CFR 63.2470(f), respectively). An opportunity to comment on the storage vessel degassing provisions was not previously provided because, based on comments received for all three rules, the provisions were included in the final 2020 rules but not in the rules proposed in 2019. Therefore, the EPA re-proposed in 2023 what was finalized for each rule in 2020. The EPA also proposed additional revisions based on petitioners' arguments to address degassing of floating roof storage vessels. The requirements, as finalized in the 2020 rules, allow storage vessels to be vented to the atmosphere once a storage vessel degassing concentration threshold is met (*i.e.*, less than 10 percent of the lower explosive limit (LEL)) and all standing liquid has been removed from the vessel to the extent practicable. The requirements are applicable to all storage vessels (regardless of roof type) that are subject to control requirements in each of the rules. We based the degassing standard on Texas permit conditions, which

represented the MACT floor.²⁵ Specifically, permit condition 6 (applicable to floating roof storage vessels) and permit condition 7 (applicable to fixed roof storage vessels) formed the basis of the storage vessel degassing standard.

The petitioners stated that while they did identify the Texas permit conditions as a reference in their comments to the 2019 proposed rules, certain key information was not incorporated into the final 2020 EMACT standards, OLD NESHAP, and MON for the degassing of floating roof storage vessels. Additionally, the petitioners argued that they did not request additional work practices for floating roof storage vessels for which owners and operators already elect to comply with the floating roof storage vessels requirements in 40 CFR part 63, subpart WW because, even with the removal of the shutdown exemption, the petitioners contended that it is still possible to comply with the subpart WW provisions.

The EPA disagreed with the petitioners' claims that a separate standard for floating roof storage vessel degassing is not needed due to the removal of the shutdown exemption. Rather, we determined that we must set a storage vessel degassing standard that applies to storage vessels under CAA section 112. We also determined that storage vessel degassing is a unique shutdown activity with operations and emissions that are completely different from normal storage vessel operations, and 40 CFR part 63, subpart WW does not address degassing emissions from floating roof storage vessels.

Because the EPA determined that a standard is necessary for degassing of all storage vessels (regardless of roof type), the EPA reviewed the Texas permit conditions again to determine if revisions to the degassing standard for floating roof storage vessels in the EMACT standards, OLD NESHAP, and MON are appropriate. Based upon this review, we proposed and are now finalizing that a floating roof storage vessel may be opened prior to degassing to set up equipment (*i.e.*, make connections to a temporary control device), but this must be done in a limited manner and operators must not actively purge the storage vessel while connections are made. See section III.B. of the preamble to the proposed rule for additional details on the storage vessel degassing revisions.²⁶

²⁵ Texas Permit Conditions are available at: <https://www.tceq.texas.gov/assets/public/permitting/air/Guidance/NewSourceReview/mss/chem-mssdraftconditions.pdf>.

²⁶ 88 FR 25581 (Apr. 27, 2023).

²⁴ 88 FR 25574, 25580 (Apr. 27, 2023).

Comments: Several commenters supported the storage vessel degassing requirements in the 2023 proposal, including having a separate requirement for floating roof storage vessels. However, some commenters requested clarification on certain aspects of the rule text. A commenter requested clarification on whether the phrase “must not be actively degassed” (from the rule text) and “not actively purge” (from the preamble) have the same meaning for floating roof storage vessels. The commenter also requested confirmation that breathing emissions following a floating roof landing and before commencing degassing operations are not a deviation of the standard. A commenter stated that not providing a timeframe for degassing creates ambiguity and encouraged the EPA to use the same 24-hour window as the Texas permit conditions for consistency. Another commenter recommended the EPA incorporate a requirement based on the maintenance vent standard, which would allow active purging if the pressure in the storage vessel is 2 pounds per square inch gauge or less. A commenter recommended that the EPA incorporate additional recordkeeping and reporting requirements for storage vessel degassing, such as recording and reporting information from the vapor space concentration measurements. A commenter also requested the EPA further define degassing.

Response: After consideration of the comments submitted, we are finalizing the storage vessel degassing requirements as proposed, including the separate requirement for floating roof storage vessels. We do confirm that the phrase “must not be actively degassed” (from the rule text) and “not actively purge” (from the preamble) have the same meaning for purposes of the floating roof storage vessel degassing provisions. We are also aware that the Texas permit condition 6.B provides a 24-hour window to start controlled degassing after the floating roof storage vessel has been drained, and that the storage vessel may be opened during this period only to set up for degassing and cleaning. However, we determined at proposal that the 24-hour window stipulates how long a floating roof storage vessel can be landed before it needs to be filled again or degassed, but it does not have a direct bearing on the underlying control standard for degassing operations. As such, we are not revising the final rule to incorporate the 24-hour window into the storage vessel degassing standard.

We agree with the commenter that emissions as a result of vapor space

expansion (*i.e.*, breathing emissions) following landing of a floating roof and prior to commencing degassing operations do not constitute a bypass or deviation of the standards. We note that this work practice standard for storage vessel degassing applies “during storage vessel shutdown operations (*i.e.*, emptying and degassing of a storage vessel).”

We also do not agree that incorporating a requirement similar to the maintenance vent standard is appropriate for storage vessel degassing. The intent of the standard is to control degassing emissions to the level of the MACT floor, which in this case is the use of controls to minimize emissions until the vapor space concentration reaches 10 percent of the LEL.

We do not believe that additional clarity on the definition of degassing is warranted as this process is well understood. Storage vessel degassing has always been in the rules as part of the definition of “Shutdown” (*i.e.*, Shutdown also applies to emptying and degassing storage vessels). In addition, there have been many commenters on each of the rules over the past four years providing feedback regarding storage vessel degassing; during this time no clarifications regarding the definition of degassing were needed.

We are finalizing clarifications to the storage vessel degassing standards for the EMACT standards at 40 CFR 63.1103(e)(10), the OLD NESHAP at 40 CFR 63.2346(a)(6), and the MON at 40 CFR 63.2470(f).

We also want to clarify that the overlap provisions in the MON and OLD NESHAP for storage vessels do not apply with respect to demonstrating compliance with the storage vessel degassing standards.²⁷ While these overlap provisions (*e.g.*, 40 CFR part 60, subpart Kb; 40 CFR part 61, subpart Y) do include storage vessel standards that facilities subject to the MON and OLD NESHAP may comply with for storage vessels during normal operation, they do not include an equivalent alternative standard to the storage vessel degassing standards that were finalized in 2020 and that are being clarified in this final action. As such, facilities subject to the MON and OLD NESHAP must always comply with the storage vessel degassing standards included therein

²⁷ The EMACT standards require owners or operators to comply specifically with the EMACT standards where overlap may exist for various storage vessel control requirements (see 40 CFR 63.1100(g)(1)); thus, it is not necessary to clarify that the storage vessel degassing standards always apply in this NESHAP.

even if complying with these overlap provisions.

C. Other EMACT Standards Technical Corrections and Clarifications

The EPA is finalizing additional revisions for the EMACT standards that address other technical corrections and clarifications and correct typographical errors. We received comments on some of the revisions that were proposed for the EMACT standards. In this section, we provide comment summaries and responses for the EMACT standards topics where comments were received. We also include revisions to the EMACT standards that were not proposed but for which commenters provided technical clarifications to the rule and the EPA is finalizing. Table 2 of this preamble shows the revisions to the EMACT standards for which no comments were received, and that the EPA is finalizing as proposed. Although we briefly summarize these items below, refer to section III.C.1. of the preamble to the proposed rule for additional details.²⁸

Topic summary, delay of burner repair provisions (40 CFR

63.1103(e)(7)(i)): A petitioner argued that requiring an ethylene cracking furnace to implement the delay of burner repair provisions finalized in the 2020 final rule is impracticable and is inconsistent with what the best performers are doing. The petitioner stated that a significant amount of preparation is needed to shutdown an ethylene cracking furnace and that no source can comply with the delay of burner repair provisions as written. Accordingly, where a burner cannot be repaired without an ethylene cracking furnace shutdown, owners or operators would have to decoke their ethylene cracking furnaces immediately (*i.e.*, within 1 day of identifying flame impingement), leading to more decoking events and subsequently more emissions from the decoking of ethylene cracking furnaces.

An opportunity to comment on the delay of burner repair provisions was not previously provided because the provisions were included in the final 2020 rule but not in the 2019 proposed rule. Therefore, the EPA re-proposed at 40 CFR 63.1103(e)(7)(i) what was finalized along with the following revisions for delay of burner repair.

The EPA proposed to remove the requirement that the owner or operator may only delay burner repair beyond 1 calendar day if a shutdown for repair would cause greater emissions than the potential emissions from delaying repair. We agreed that this requirement

²⁸ 88 FR 25582 (Apr. 27, 2023).

if left in place would lead to more decoking events and more emissions from decoking of ethylene cracking furnaces. Instead of evaluating emissions to determine whether delay of repair is allowed, the EPA proposed that delay of repair beyond 1 calendar day is allowed if the repair cannot be completed during normal operations, the burner cannot be shutdown without significantly impacting the furnace heat distribution and firing rate, and action is taken to reduce flame impingement as much as possible during continued operation. We also maintained that if a delay of repair is required to fully resolve burner flame impingement, repair must be completed following the next planned decoking operation (and before returning the ethylene cracking furnace back to normal operation) or during the next ethylene cracking furnace complete shutdown (when the ethylene cracking furnace firebox is taken completely offline), whichever is earlier.

Comments: A few commenters supported the proposed revision to the ethylene cracking furnace delay of burner repair requirements. They indicated that the proposed language provided needed flexibility. However, some of the commenters recommended additional revisions to the language to add specificity regarding when burner repair is allowed. Specifically, the commenters asked for an allowance to delay repairs until the next planned shutdown if a complete furnace shutdown is required to complete the repair.

Response: We disagree with the commenters that additional allowances for burner repair are warranted and are finalizing the revisions as proposed. We proposed the revisions to the delay of repair language to provide flexibility and acknowledge the industry's general practice for burner inspection and repair. However, allowing facilities to protract burner repair to a further point in time, which may be years in the future for the next ethylene cracking furnace complete shutdown, goes against the purpose of the burner inspection and repair provisions which is to stop flame impingement and minimize decoking emissions. Additionally, the decoking of ethylene cracking furnaces has always been included in the definition of *Shutdown* in the regulatory text of the EMACT standards and has always been considered a shutdown operation. The EPA is finalizing the delay of burner repair provisions as proposed and owners or operators must repair the burner following the next decoking

event or complete shutdown, whichever is earlier.

Topic summary, isolation valve inspection and repair (40 CFR 63.1103(e)(8)(i)): A petitioner requested that the EPA revise the requirement to rectify poor isolation prior to continuing decoking operations. The petitioner argued that certain isolation valve repairs must be completed after the ethylene cracking furnace is shutdown, which consequently requires decoking the ethylene cracking furnace. The petitioner said that if a furnace is not decoked prior to shutdown, damage can occur to the furnace tubes and could pose a safety issue. In addition, the petitioner noted that some isolation valves serve gas streams from multiple ethylene cracking furnaces, and there may be instances when all furnaces would need to be decoked and shutdown to properly rectify the isolation valve issue. The petitioner argued that allowing for some flexibility is necessary for facilities to operate properly and to avoid damaging equipment.

We agreed with the petitioner and proposed language at 40 CFR 63.1103(e)(8)(i) to allow facilities to wait and rectify isolation valve issues after a decoking operation, provided that the owner or operator can reasonably demonstrate that damage to the radiant tube(s) or ethylene cracking furnace would occur if the repair was attempted prior to completing a decoking operation and/or prior to the ethylene cracking furnace being shutdown.

Comments: Some commenters supported the proposed revision to the ethylene cracking furnace isolation valve inspection and repair requirements. They indicated that the proposed language was consistent with industry practices. The commenters also recommended additional revisions to emphasize that the company must be able to make the determination regarding whether to delay repair if the radiant tubing or ethylene cracking furnace could be damaged.

Response: The EPA acknowledges the commenters' support and is revising the proposed language in response to the comments. We agree that the owner or operator does not need to directly demonstrate to the regulating authority that damage would occur to the radiant tubes or ethylene cracking furnace before using the allowance to delay repair. We are clarifying in 40 CFR 63.1103(e)(8)(i) that the owner or operator can make the determination that damage could occur in order to avail themselves of this delay of repair allowance.

Topic summary, removal of electronic reporting requirements (40 CFR 63.1100(b), 63.1103(e)(4)(iii), and 63.1110(a)(10)(i), (ii), (iii), and (iv)): Instructions for submitting reports electronically through CEDRI, including instructions for submitting CBI and asserting a claim of EPA system outage or *force majeure*, were recently added to 40 CFR 63.9(k);²⁹ therefore, text related to these requirements was no longer necessary in the EMACT standards. As such, we removed duplication and pointed directly to 40 CFR 63.9(k) when required to submit certain reports to CEDRI.

Comment: A commenter agreed with the revisions to point to 40 CFR 63.9(k) directly, but also stated that an additional reference to this citation is warranted in 40 CFR 63.1100(b).

Response: We agree with the commenter and are referencing 40 CFR 63.9(k) in the last sentence of 40 CFR 63.1100(b). We are also finalizing the edits at 40 CFR 63.1103(e)(4)(iii) and 63.1110(a)(10)(i), (ii), (iii), and (iv), as proposed.

Topic summary, LEL clarification (40 CFR 63.1103(e)(5), 63.1103(e)(10), 63.1109(f), 63.1110(e)(5)): These provisions reference the term "LEL" for the purposes of determining compliance. We did not propose revisions for this term, but commenters provided feedback stating that it was being misused.

Comments: Commenters stated that we were misusing the term LEL in certain rule provisions for maintenance vents and storage vessel degassing (e.g., 40 CFR 63.1103(e)(5), 40 CFR 63.1103(e)(10)). Commenters stated the LEL was a fixed physical property of a vapor mixture and thus, is neither changed nor measured. According to commenters, LEL refers to a specific concentration value for a particular mixture. For example, when opening a maintenance vent, commenters elaborated that you measure the concentration of the vapor and then you can compare that concentration to the LEL. The commenter thought the rule text incorrectly implied that you measured the LEL of the vapor. The commenters requested that the EPA clarify that the concentration of the vapors in equipment for maintenance vents (and the vapor space concentration for storage vessel degassing) must be less than 10 percent of the LEL and that facilities are to measure the concentration, not the LEL.

Response: We agree with commenters that the rule text referring to the LEL was used incorrectly for certain

²⁹ 85 FR 73885 (Nov. 19, 2020).

maintenance vent and storage vessel degassing provisions and that the LEL cannot be changed for a vapor. We are

revising the rule text to make clear that facilities measure the vapor concentration and then compare that

concentration value to the LEL of the vapor to determine if the concentration is less than 10 percent of the LEL.

TABLE 2—SUMMARY OF REVISIONS TO 40 CFR PART 63, SUBPART YY FOR WHICH THE EPA RECEIVED NO COMMENT

Provision	Issue summary	Final revision
40 CFR 63.1110(e)(4)(iii)	Provision contains a typographical error.	The EPA is replacing “§ 63.1109(e)(7)” with “§ 63.1109(e)(6)” to correct the typographical error.
40 CFR 63.1102(c)(11), (d)(2)(ii), and (e)(2)(iii).	Provisions contain a typographical error.	The EPA is replacing “§ 63.1108(a)(4)(i)” with “§ 63.1108(a)(4)” to correct a typographical error that we made while removing startup, shutdown, and malfunction exemptions.

D. Other OLD NESHAP Technical Corrections and Clarifications

There are additional revisions that we are finalizing for the OLD NESHAP to address other technical corrections and clarifications and to correct

typographical errors. We did not receive comments on all of the revisions that were proposed for the OLD NESHAP. Table 3 of this preamble shows the revisions to the OLD NESHAP for which no comments were received and the EPA is finalizing as proposed. Table 4

of this preamble shows revisions to the OLD NESHAP which were not proposed but where commenters provided technical clarifications to the rule, which the EPA is finalizing. Refer to section III.C.2. of the preamble to the proposed rule for additional details.³⁰

TABLE 3—SUMMARY OF REVISIONS TO 40 CFR PART 63, SUBPART EEEE FOR WHICH THE EPA RECEIVED NO COMMENT

Provision	Issue summary	Final revision
40 CFR 63.2346(a)(6)	Provision contains a typographical error	The EPA is replacing “items 3 through 6 of table 2 to this subpart” with “items 2 through 6 of table 2 to this subpart” to correct the typographical error.
40 CFR 63.2346(e)	Provision contains a typographical error	The EPA is replacing “storage vessels” with “storage tanks” to correct the typographical error.
40 CFR 63.2378(e)(3)	Provision needing technical clarifications	The EPA is adding the word “planned” in front of “routine maintenance” in the last sentence of the provision in order to further clarify the provision only applies to periods of planned routine maintenance. We are also replacing “storage vessel” with “storage tank” in the last sentence of the provision to correct a typographical error.
40 CFR 63.2378(e)(4)	Provision needing technical clarifications	To create consistency in the time period during which the bypass provision applies (<i>i.e.</i> , the level of material in the storage vessel must not be increased during the same time period that breathing loss emissions bypass the fuel gas system or process), we are deleting “to perform routine maintenance” from the last sentence of 40 CFR 63.2378(e)(4). We are also replacing “storage vessel” with “storage tank” in the last sentence of the provision to correct a typographical error.
40 CFR 63.2382(d)(3); 63.2386(f), (g), (h), (i), and (j); and 63.2406.	Provisions needing technical clarifications or removal ...	The EPA is removing duplication and pointing directly to 40 CFR 63.9(k) when required to submit certain reports to CEDRI. Specifically, instructions for submitting reports electronically through CEDRI, including instructions for submitting CBI and asserting a claim of EPA system outage or <i>force majeure</i> , were recently added to 40 CFR 63.9(k) (85 FR 73885; November 19, 2020); therefore, text related to these requirements was no longer necessary in the OLD NESHAP.

³⁰ 88 FR 25584 (Apr. 27, 2023).

TABLE 4—SUMMARY OF REVISIONS TO 40 CFR PART 63, SUBPART EEEE THAT WERE NOT PROPOSED BUT ARE BEING FINALIZED BASED ON COMMENTER INPUT

Provision	Issue summary	Final revision
40 CFR 63.2346(a)(6)	In comments on the EMACT standards, MON, and Petroleum Refinery MACT 1, commenters stated that we were misusing the term LEL in certain rule language provisions for maintenance vents and storage vessel degassing. See the comment summary and response in section III.C. of this preamble for additional details.	While commenters did not specifically point out revisions to the OLD NESHAP, we are finalizing revisions to 40 CFR 63.2346(a)(6) for consistency. Specifically, we are clarifying that the owner or operator must determine the concentration of the vapor space as opposed to determining the LEL of the vapor space.
Table 12 to Subpart EEEE of Part 63.	Provisions needing technical clarifications	40 CFR 63.7(a)(4) is not cited in the general provisions applicability table. We are referencing 40 CFR 63.7(a)(4) in this table and stating it applies to the OLD NESHAP.

E. Other MON Technical Corrections and Clarifications

This section of the preamble presents revisions we are finalizing to the MON heat exchange system requirements along with additional revisions that we are finalizing for the MON to address other technical corrections and clarifications and to correct typographical errors. We did not receive comments on some of the revisions that were proposed for the MON. In this section, we provide comment summaries and responses for the MON topics where comments were received. We also include revisions to the MON which were not proposed but where commenters provided technical clarifications to the rule, which the EPA is finalizing. Following this, table 5 of this preamble shows the revisions to the MON for which no comments were received, and the EPA is finalizing as proposed. We briefly summarize these items below; see section III.C.3. of the preamble to the proposed rule for additional details.³¹

Topic summary, leak monitoring requirements for heat exchange systems with soluble HAP (40 CFR 63.2490(e)): In May 2021, EPA Region 4 received a request from Eastman Chemical Company to perform alternative monitoring instead of the Modified El Paso Method to monitor for leaks in Eastman’s Tennessee Operations heat exchange systems, which primarily have cooling water containing soluble HAP with a high boiling point (see Docket Item No. EPA–HQ–OAR–2022–0787–0028). Eastman requested that the previous water sampling requirements for heat exchange system leaks provided in the MON, which ultimately references 40 CFR 63.104(b) (*i.e.*, use of any EPA-approved method listed in 40 CFR part 136 as long as the method is sensitive to concentrations as low as 10 parts per million (ppm) and the same

method is used for both entrance and exit samples), be allowed for cooling water containing certain soluble HAP in lieu of using the Modified El Paso Method. Eastman specifically identified two HAP, 1,4-dioxane and methanol, which do not readily strip out of water using the Modified El Paso Method. Eastman’s application for alternative monitoring included experimental data showing that the Modified El Paso Method would likely not identify a leak of these HAP in heat exchange system cooling water. Based upon a review of the information provided by Eastman, we proposed that water sampling of heat exchange systems may be used but only if 99 percent by weight or more of all the organic compounds that could potentially leak in the cooling water have a Henry’s Law Constant less than a certain threshold (*i.e.*, 5.0E–6 atmospheres per mole per cubic meter (atm-m³/mol) at 25° Celsius). See section III.C.3. of the preamble to the proposed rule for additional details.³²

Comments: Some commenters supported the proposed revisions to allow for water sampling of heat exchange systems, instead of the Modified El Paso Method, in limited instances. However, each of the commenters also argued that the EPA must revise the proposed language to add specificity regarding the compounds for which the water sampling alternative could be used. The commenters stated that the requirement should only apply to heat exchange systems with 99 percent by weight or more of organic HAP compounds that meet certain thresholds instead of just 99 percent by weight or more of organic compounds that meet certain thresholds. The commenters contended that because the rule serves to identify leaks of HAP, specifying that the threshold applies only to organic HAP is necessary. The commenters were

concerned the proposed revisions could lead to expenditures fixing leaks that do not contain HAP. A commenter also requested the EPA clarify whether small heat exchange systems with a cooling water flow rate of 10 gallons per minute or less are required to use the Modified El Paso Method.

Response: After considering the comments submitted, the EPA is finalizing the monitoring revisions as proposed to allow for water sampling of heat exchange systems in limited instances. We disagree with the commenters’ request to revise the language to specify “HAP” compounds for the 99 percent by weight requirement. The proposed revisions do not impact what heat exchangers are subject to monitoring; rather they help determine what type of monitoring is allowed (*i.e.*, Modified El Paso Method or water sampling), and the existing language already includes specificity regarding HAP compounds. The definition of heat exchange system states that the heat exchange system must be in organic HAP service (*i.e.*, contain at least 5 percent by weight of total organic HAP) in order to be subject to the heat exchange system monitoring requirements. Additionally, 40 CFR 63.104(b) is clear that owners and operators must monitor for “the presence of one or more organic hazardous air pollutants or other representative substances whose presence in cooling water indicates a leak.” The introductory text of 40 CFR 63.2490(e), which says: “you may monitor the cooling water for leaks according to the requirements in § 63.104(b) in lieu of using the Modified El Paso Method,” is also only intended to specify what type of monitoring is required.

Regarding small heat exchange systems with a cooling water flow rate of 10 gallons per minute or less, we believe that further clarification to the rule is not needed. The 10 gallons per

³¹ 88 FR 25584 (Apr. 27, 2023).

³² 88 FR 25584 (Apr. 27, 2023).

minute threshold provided in 40 CFR 63.2490(d) only applies to the Modified El Paso Method monitoring requirements in 40 CFR 63.2490(d). As such, heat exchange systems with a cooling water flow rate of 10 gallons per minute or less are still subject to the requirements of 40 CFR 63.104, as they have been historically, and must continue complying as they always have.

In summary, the EPA is finalizing at 40 CFR 63.2490(e) that the leak monitoring requirements for heat exchange systems at 40 CFR 63.104(b) may be used in limited instances (*i.e.*, if 99 percent by weight or more of all the organic compounds that could potentially leak into the cooling water have a Henry's Law Constant less than $5.0E-6$ atmospheres per mole per cubic meter ($\text{atm}\cdot\text{m}^3/\text{mol}$) at 25° Celsius) instead of using the Modified El Paso Method to monitor for leaks. While we are finalizing that the leak monitoring and leak definition requirements at 40 CFR 63.104(b) may be used in limited instances, we did not propose nor finalize that other provisions of 40 CFR 63.104 apply. Instead, for example, facilities that use water sampling to detect leaks must still comply with the recordkeeping and reporting requirements of 40 CFR 63.2520(e)(16) and 40 CFR 63.2525(r). We are finalizing revisions at 40 CFR 63.2520(e)(16) and 40 CFR 63.2525(r) to specify this.

Topic summary, PRDs with rupture disks (40 CFR 63.2480(e)(2)(ii) and (e)(2)(iii)): For PRDs with rupture disks, a petitioner pointed out that EPA agreed in their response to comment document (see docket item EPA-HQ-OAR-2018-0746-0200 in the MON RTR docket) to delete the second sentence (*i.e.*, the requirement to conduct monitoring if rupture disks are replaced) from 40 CFR 63.2480(e)(2)(ii) and (e)(2)(iii). However, the final rule (85 FR 49084, August 12, 2020) did not reflect these deletions. We agreed that the language diverges from what 40 CFR part 63, subpart UU required for PRDs. Therefore, we proposed to correct this error by deleting the second sentence from 40 CFR 63.2480(e)(2)(ii) and (e)(2)(iii).

Comments: A commenter supported the proposed revision to the monitoring requirements for PRDs with rupture disks and stated the revision provides consistency with other rules.

Response: The EPA acknowledges the commenter's support, and we are finalizing the revisions as proposed.

Topic summary, scrubber testing and monitoring requirements (40 CFR 63.2493(a)(2)(vi) and (b)(4)): A petitioner requested clarification of scrubber monitoring parameters and the

types of scrubbers that are applicable to certain requirements at 40 CFR 63.2493(a)(2)(vi) and (b)(4). The petitioner stated that the rule is only applicable to scrubbers that use an acid solution and reactant tank, but that other types of scrubbers are used in instances when ethylene oxide is present in small amounts. The petitioner requested the pH monitoring parameter be revised to account for other types of scrubbers. The petitioner also requested the temperature of the "scrubber liquid" be monitored instead of the temperature of the "water."

Scrubbers that use an acid solution and reactant tank are the primary focus of the scrubber monitoring requirements because this type of scrubber liquid is necessary to specifically control ethylene oxide. As such, we did not propose to revise the monitoring parameters to apply more broadly, such as to scrubbers that use water as the scrubbing liquid. We proposed clarifying language that the monitoring requirements at 40 CFR 63.2493(a)(2)(vi) and (b)(4) are applicable to scrubbers "with a reactant tank." We agreed with the petitioner regarding temperature monitoring and proposed a correction that the temperature of the "scrubber liquid" must be monitored. We also proposed clarifying language at 40 CFR 63.2493(a)(2)(viii) and (b)(6), that if a facility uses a scrubber without a reactant tank that provides control of ethylene oxide, the facility may establish site-specific operating parameters.

Comments: Commenters supported the proposed revision to the scrubber testing and monitoring requirements for scrubbers controlling ethylene oxide. In addition, a commenter recommended that the EPA only allow scrubbers with reactant tanks and acid solutions to control ethylene oxide. Another commenter also requested that the EPA allow any scrubber to control ethylene oxide by developing site-specific operating parameters, regardless of the amount of control the scrubber provides. This commenter stated they understood the proposal allows for site-specific operating parameters only if the scrubber provides incidental control of ethylene oxide.

Response: We acknowledge the commenters' support and are finalizing the revisions as proposed. The EPA notes that in the proposed regulatory text changes for the MON, we did not use the phrase "incidental control." We are clarifying provisions at 40 CFR 63.2493(a)(2)(viii) and (b)(6), which would allow an owner or operator who uses a scrubber without a reactant tank to request appropriate operating

parameters from the Administrator. In the preamble of the proposed rule, we noted that this option would be available to facilities using scrubbers for incidental control, because it is likely that a scrubber needing to control a significant quantity of ethylene oxide emissions would need to be equipped with a reactant tank. It is unlikely that a water scrubber could provide adequate control of significant ethylene oxide emissions.

Consistent with our long-standing approach of allowing regulated industries to determine how to meet numeric emission limits, the EPA is not requiring the use of acid scrubbers for the control of ethylene oxide. Currently, scrubbers with acid solutions are likely the only scrubber technology that can achieve significant control of ethylene oxide; however, we also acknowledge that there are some facilities with ethylene oxide emissions that are very low and almost meet the outlet concentration limit without control. These owners and operators should be able to use any control device that can allow them to achieve the emission standard. Additionally, there could be a development of new scrubbing technologies for ethylene oxide in the future that use a configuration other than acid solutions and a reactant tank. We do not want to limit the development of these technologies by limiting the control devices that owners and operators must use.

Topic summary, storage tank ethylene oxide concentration (40 CFR 63.2492(b)): A petitioner requested that an alternative to sampling and analysis of storage tank materials should be allowed, to determine if a storage tank is in ethylene oxide service. The petitioner stated that information already exists for some storage tanks to show that the ethylene oxide concentration in the material stored is less than 0.1 percent by weight (sometimes significantly so) and that it is unnecessary to require sampling and analysis. We agreed with the petitioner and proposed to amend 40 CFR 63.2492(b) to allow calculations to be performed to show that the ethylene oxide concentration is less than 0.1 percent by weight of the material stored in the storage tank, provided the calculations rely on information specific to the material stored. This may include using, for example, specific concentration information from safety data sheets.

Comments: Commenters supported the proposed revision to allow calculations to determine the ethylene oxide concentration of the fluid stored in a storage tank. A commenter also

recommended that the EPA expand this requirement and allow the use of engineering judgement and process knowledge to determine the concentration, similar to what is allowed to determine the ethylene oxide content for equipment leaks.

Another commenter did not support the proposed revision to allow calculations to determine the ethylene oxide concentration of the fluid stored in a storage tank. The commenter argued that calculations introduce uncertainty and are often underestimated.

A commenter also noted that proposed 40 CFR 63.2492(b)(i) and (b)(ii) should be renumbered to 40 CFR 63.2492(b)(1) and (b)(2).

Response: We are finalizing the revisions to allow calculations to determine the ethylene oxide concentration of the fluid stored in a storage tank as proposed. We disagree with the commenter's request to add more flexibility to the alternative approach in 40 CFR 63.2492(b)(2) for storage tanks to be consistent with the equipment leaks provision at 40 CFR 63.2492(c)(2). The rule is already clear regarding determining whether storage tanks are "in ethylene oxide service." In order to determine the requirements for storage tanks in ethylene oxide service, facilities must look at both the definition of "in ethylene oxide service" and the requirements in 40 CFR 63.2492 together. The definition of "in ethylene oxide service" lets the owner or operator designate a storage tank based on process knowledge; however, if an owner or operator wants to say a storage tank is not in ethylene oxide service, they must use the procedures in 40 CFR 63.2492(b). The rule at 40 CFR 63.2492(b)(2) already explicitly allows for an owner or operator to calculate the concentration of ethylene oxide of the fluid stored in a storage tank if information specific to the fluid stored is available which includes data based on safety data sheets.

We do agree with the commenter that the proposed numbering was incorrect and are finalizing the revisions at 40 CFR 63.2492(b)(1) and (b)(2).

We are also changing the phrasing of "sampling and analysis is performed as specified in § 63.2492" to "the procedures specified in § 63.2492 are performed" within the definition of "in ethylene oxide service" for storage tanks. This language more clearly aligns with the revised requirements at 40 CFR 63.2492(b).

Topic summary, delay of repair provisions for equipment in ethylene oxide service (40 CFR 63.2493(d)(1)(iii) and 63.2493(d)(2)(iii)): A petitioner

requested the EPA clarify whether delay of repair provisions apply to equipment in ethylene oxide service. The petitioner noted that in the response to comments for the final rule, the EPA stated that delay of repair provisions do not apply. However, the petitioner further noted the final rule language did not reflect this. We proposed to revise 40 CFR 63.2493(e) to specify that the delay of repair provisions of 40 CFR part 63, subparts H and UU and 40 CFR part 65, subpart F do not apply for all equipment in ethylene oxide service.

Comments: Commenters did not support the proposed revision to remove the delay of repair provisions for equipment in ethylene oxide service. The commenters contended that removing the delay of repair provisions would increase emissions, because the emissions due to shutdowns can be higher than the leak emissions due to invoking delay of repair. This is particularly true if few components are leaking. A commenter emphasized that companies consider both worker safety and emissions when evaluating leaks and noted some companies have ambient air monitors for ethylene oxide. The commenters stated the number of components in ethylene oxide service that leak is low, and that this is supported by data submitted by chemical manufacturing facilities (which are similar to MON facilities) to the EPA which indicated no leaking connectors, valves, or pumps in ethylene oxide service. The commenters also stated the delay of repair provisions provide important flexibility for companies and allow them to operate without disruptions to their operations.

Another commenter supported the proposed revision to remove the delay of repair provisions for equipment in ethylene oxide service.

Response: We partly erred when stating at proposal that the MON included delay of repair provisions for equipment in ethylene oxide service. The final 2020 MON included specific repair requirements for pumps and connectors in ethylene oxide service at 40 CFR 63.2493(d)(1)(iii) and 63.2493(d)(2)(iii), respectively. These requirements stipulated that a leak must be repaired within 15 days after it is detected. No exceptions were provided for the 15-day timeframe, which means there were no exceptions for delay of repair. Other equipment in ethylene oxide service (e.g., valves) do not have ethylene oxide-specific requirements in the MON like connectors and pumps, and it was our intent that delay of repair provisions still apply for this other

equipment (i.e., reducing ethylene oxide emissions from connectors and pumps was determined to be necessary for the 2020 rule, and thus delay of repair was not provided for them). As such, we are not revising the MON to exclude delay of repair provisions for equipment other than connectors and pumps in ethylene oxide service and are not finalizing the revision that was proposed at 40 CFR 63.2493(e)(17). We are maintaining the existing requirements at 40 CFR 63.2493(d)(1)(iii) and 63.2493(d)(2)(iii), with one additional revision. We are finalizing a revision that allows for the delay of repair for connectors and pumps in ethylene oxide service if the equipment is isolated from the process and does not remain in ethylene oxide service.

Topic summary, LEL clarification (40 CFR 63.2450(v), 63.2470(f), 63.2520(e)(14), 63.2525(p)): Maintenance vent and storage vessel degassing provisions reference the term LEL to determine compliance. We did not propose revisions to this term, but commenters provided feedback stating it was being misused.

Comments: Commenters stated that we were misusing the term LEL in certain rule language provisions for maintenance vents and storage vessel degassing (e.g., 40 CFR 63.2450(v), 40 CFR 63.2470(f)). Commenters stated the LEL was a fixed physical property of a vapor mixture and thus does not change nor is it measured. It refers to a specific concentration value for a particular mixture. For example, commenters explained that, when opening a maintenance vent, the concentration of the vapor is measured and then compared to the LEL. The rule text incorrectly implied that the LEL of the vapor is measured. The commenters requested that the EPA clarify that the concentration of the vapors in equipment for maintenance vents (and the vapor space concentration for storage vessel degassing) must be less than 10 percent of the LEL and that facilities are to measure the concentration, not the LEL.

Response: We agree with commenters that the rule text referring to the LEL was used incorrectly for certain maintenance vent and storage vessel degassing provisions and that the LEL cannot be changed for a vapor. We are revising the rule text to be clear that facilities measure the vapor concentration and then compare that concentration value to the LEL of the vapor to determine if the concentration is less than 10 percent of the LEL.

TABLE 5—SUMMARY OF REVISIONS TO 40 CFR PART 63, SUBPART FFFF FOR WHICH THE EPA RECEIVED NO COMMENT

Provision	Issue summary	Final revision
40 CFR 63.2450(e)(6)(i)	Provision contains a typographical error	The EPA is replacing the reference to 40 CFR 63.148(h)(3) with a reference to 40 CFR 63.148(i)(3) to correct the typographical error.
40 CFR 63.2450(e)(7)	A petitioner requested that the EPA clarify whether certain adsorber provisions referenced within 40 CFR 63.983 and other related requirements and exceptions (<i>i.e.</i> , 40 CFR 63.2470(c)(3), 40 CFR 63.2520(d)(6) and (e)(13), and 40 CFR 63.2525(o)) apply to this paragraph. The petitioner also pointed out that it is not clear whether a supplement to the notification of compliance status (NOCS) report is needed, and if necessary, what information should be provided.	The EPA is clarifying that 40 CFR 63.2470(c)(3), 40 CFR 63.2520(d)(6) and (e)(13), 40 CFR 63.2525(o), and the provisions referenced within 40 CFR 63.983 all apply (in addition to 40 CFR 63.2450(e)(4) and (e)(6)) if facilities reduce organic HAP emissions by venting emissions through a closed-vent system to an adsorber(s) that cannot be regenerated or a regenerative adsorber(s) that is regenerated offsite. We are also clarifying in 40 CFR 63.2450(e)(1) that 40 CFR 63.2450(e)(1) does not apply when complying with 40 CFR 63.2450(e)(7). As part of this clarification, we are also finalizing a new requirement at 40 CFR 63.2520(d)(6) for adsorbers subject to the requirements of 40 CFR 63.2450(e)(7) requiring a supplement to the NOCS report within 150 days after the first applicable compliance date. We are finalizing that the supplement to the NOCS report must describe whether the adsorber cannot be regenerated or is a regenerative adsorber(s) that is regenerated offsite; and specify the breakthrough limit and adsorber bed life that was established during the initial performance test or design evaluation of the adsorber. Finally, we are revising the introduction paragraph of 40 CFR 63.2520 as well as the requirement in 40 CFR 63.2515(d) to update the reference to 40 CFR 63.2520(d)(6).
40 CFR 63.2460(c)(9)	Provision contains a typographical error	The EPA is replacing the phrase “in paragraphs (c)(9)(i) through (vi) of this section” with “in paragraphs (c)(9)(i) through (iv) of this section” to correct the typographical error.
40 CFR 63.2480(a)	Provision contains a typographical error	The EPA is replacing the phrase “For each light liquid pump, valve, and connector in ethylene oxide service” with “For each light liquid pump, pressure relief device, and connector in ethylene oxide service” to correct the typographical error.
40 CFR 63.2480(f)(18)(iii)	Provision contains a typographical error	The EPA is replacing “§63.181(b)(2)(i)” with “§63.181(b)(3)(i)” to correct the typographical error.
40 CFR 63.2480(f)(18)(vi)	A petitioner contended that the reference to information required to be reported under 40 CFR 63.182(d)(2)(xiv) is too broad and should be more narrowly described as “information in §63.165(a) required to be reported under 40 CFR 63.182(d)(2)(xiv)” in order to clarify that the reporting requirement is specific to the recently promulgated PRD requirements.	We agree with the petitioner that the provision should be revised to clarify that the reporting requirement is specific to the recently promulgated PRD requirements. Therefore, we are finalizing language that reads “The information in §63.165(a) required to be reported under 40 CFR 63.182(d)(2)(xiv) is now required to be reported under §63.2520(e)(15)(i) through (iii).”
40 CFR 63.2480(f)(18)(x)	Provision contains a typographical error	The EPA is replacing “§63.1022(a)(1)(v)” with “§63.1023(a)(1)(v)” to correct the typographical error.
40 CFR 63.2480(f)(18)(xiii) ..	A petitioner contended that the reference to information required to be reported under 40 CFR 63.1039(b)(4) is too broad and should be more narrowly described as “information in §63.1030(b) required to be reported under 40 CFR 63.1039(b)(4)” in order to clarify that the reporting requirement is specific to the recently promulgated PRD requirements.	We agree with the petitioner that the provision should be revised to clarify that the reporting requirement is specific to the recently promulgated PRD requirements. Therefore, we are finalizing language that reads “The information in §63.1030(b) required to be reported under 40 CFR 63.1039(b)(4) is now required to be reported under §63.2520(e)(15)(i) and (ii).”
40 CFR 63.2493(b)(2)	A petitioner requested that the EPA include introductory language to clarify that the requirements apply only if the facility chooses to route emissions to a non-flare control device and chooses to comply with the 1 parts per million volume (ppmv) standard via continuous emission monitoring systems (CEMS).	We agree with the petitioner that 40 CFR 63.2493(b)(2) only applies if the facility chooses to route emissions to a non-flare control device and chooses to comply with the 1 ppmv standard via CEMS. Therefore, we are adding introductory text at 40 CFR 63.2493(b)(2) that clarifies this.
40 CFR 63.2493(d)(3)	A petitioner contended that the reference to “affected source” should be revised to “MCPU” to be consistent with the second column of Table 6 to Subpart FFFF of Part 63.	We agree with the petitioner to revise the provision for consistency with Table 6 to Subpart FFFF of part 63; therefore, we are replacing “affected source” with “MCPU”.
40 CFR 63.2493(d)(4)(v)	Provision contains a typographical error	The EPA is replacing “§63.2445(h)” with “§63.2445(i)” to correct the typographical error.

TABLE 5—SUMMARY OF REVISIONS TO 40 CFR PART 63, SUBPART FFFF FOR WHICH THE EPA RECEIVED NO COMMENT—Continued

Provision	Issue summary	Final revision
40 CFR 63.2520(d)	A petitioner pointed out that the EPA indicated in the preamble to the final rule (85 FR 49084; August 12, 2020) that electronic reporting is required at 40 CFR 63.2520(d) for the NOCS report; however, the final rule does not contain this requirement. The petitioner requested that the EPA clarify that this was a misstatement in the preamble language and that the NOCS report is not required to be submitted electronically.	We acknowledge there was an inconsistency in what we said in the preamble about electronic reporting NOCS reports versus what we required in the 2020 final rule. However, the inconsistency is irrelevant because in this rulemaking, we are finalizing at 40 CFR 63.2520(d) to require NOCS reports be submitted electronically through the EPA's CDX CEDRI. The requirement to submit NOCS reports electronically will increase the ease and efficiency of data submittal and data accessibility.
40 CFR 63.2525(o)	A petitioner requested that the EPA update the recordkeeping requirements for adsorbers that cannot be regenerated and for regenerative adsorbers that are regenerated offsite to reflect the monitoring requirements in the final rule (85 FR 49084; August 12, 2020). Specifically, the petitioner requested that the EPA revise 40 CFR 63.2525(o)(1) to require that you must keep records of the breakthrough limit and bed life for each adsorber established according to 40 CFR 63.2450(e)(7)(i); revise 40 CFR 63.2525(o)(2) to require that you keep records of each outlet HAP or TOC concentration measured according to 40 CFR 63.2450(e)(7)(ii) and (e)(7)(iii); and revise 40 CFR 2525(o)(3) to require records of the date and time each adsorber is replaced. The petitioner also requested the EPA remove the requirement at 40 CFR 63.2525(o)(4) in its entirety.	In the 2020 final rule, we inadvertently did not revise the recordkeeping requirements to reflect the associated monitoring requirements in 40 CFR 63.2450(e)(7) (for adsorbers that cannot be regenerated and for regenerative adsorbers that are regenerated offsite). We are correcting this by revising 40 CFR 63.2525(o)(1) and (2) and removing the requirement at 40 CFR 63.2525(o)(4) in its entirety, as recommended by the petitioner. However, we are not revising 40 CFR 63.2525(o)(3) as requested by the petitioner. We are keeping the language of 40 CFR 63.2525(o)(3) as-is, which aligns with the language used in 40 CFR 63.2450(e)(7)(iii)(B).
40 CFR 63.2520(e)(2) 40 CFR 63.2450(e)(5)(iv), 63.2520(e), (f), (g), (h), and (i).	Provision contains a typographical error Provisions needing technical clarifications or removal ...	The EPA is correcting the spelling of “paragraph.” The EPA is removing duplication and pointing directly to 40 CFR 63.9(k) when required to submit certain reports to CEDRI. Specifically, instructions for submitting reports electronically through CEDRI, including instructions for submitting CBI and asserting a claim of EPA system outage or <i>force majeure</i> , were recently added to 40 CFR 63.9(k) (85 FR 73885; November 19, 2020), therefore, text related to these requirements is no longer necessary in the MON.

F. Other Petroleum Refinery MACT 1 Technical Corrections and Clarifications

There are additional revisions that we are finalizing for the Petroleum Refinery MACT 1 to address other technical corrections and clarifications and to correct typographical errors. Refer to section III.C.4. of the preamble to the proposed rule for the additional details.³³

Issue summary, pressure-assisted flares (40 CFR 63.641, 63.655, and 63.670): We proposed amendments to Petroleum Refinery MACT 1 that are consistent with flaring provisions in other recent rules (*i.e.*, EMACT standards) that adopted the Petroleum Refinery MACT 1 flare requirements but addressed additional issues, such as adding provisions for pressure-assisted flares. The proposed amendments include adding pressure-assisted flares to the definition of the term “flare” in 40 CFR 63.641 and adding appropriate requirements for pressure-assisted flares

in 40 CFR 63.670. These amendments are consistent with the EPA’s intention that all types of flares, including pressure-assisted flares, are covered by the provisions in Petroleum Refinery MACT 1. The proposed amendments for pressure-assisted flares include pilot flame standards and requirements for cross-lighting in 40 CFR 63.670(b), pressure monitoring in 40 CFR 63.670(d)(3), higher combustion zone operating limits in 40 CFR 63.670(e), and requirements to use only the direct calculation methods for determining the flare vent gas net heating value according to 40 CFR 63.670(l)(5)(ii). We also proposed reporting and recordkeeping requirements specific to pressure-assisted flares in 40 CFR 63.655(g)(11)(iii) and (i)(9)(vi), respectively.

Comment: Two commenters supported the proposed revisions for pressure-assisted flare requirements. A commenter stated the proposed revisions would reduce burden on the regulated facilities, permitting authorities, and the EPA. Another

commenter requested clarification on whether existing AMELs would be affected and whether owners and operators could still request an AMEL in the future.

Response: The EPA acknowledges the commenters’ support and we are finalizing the revisions as proposed. We confirm that owners and operators can still request an AMEL to demonstrate appropriate flare combustion efficiency, if so desired by an owner or operator. The proposed revisions did not impact the AMEL requirements of 40 CFR 63.670(r). We also confirm that existing AMELs are unaffected by the proposed revisions to the NESHAP requirements.

Topic summary, flare gas composition monitoring requirements (40 CFR 63.671): To provide additional flexibility to the monitoring requirements for flare gas composition as required by 40 CFR 63.670(j), we proposed to add mass spectrometry as a method in 40 CFR 63.671. The current provisions in 40 CFR 63.671 could be interpreted to suggest that gas chromatographs must be used for flare

³³ 88 FR 25587 (Apr. 27, 2023).

gas compositional analysis. This was not our intent. We recognize that there are some methods, like mass spectrometry, which can determine flare gas composition without the use of a gas chromatograph. We proposed to add specific requirements for calibration and operation of mass spectrometers that parallel the requirements for gas chromatographs.

Comment: One commenter provided specific rule text edits to multiple provisions within 40 CFR 63.671(e) and (f). The commenter recommended including language specific to “gas chromatograph” in 40 CFR 63.671(e); adding reference to the seven-day calibration error test period in 40 CFR 63.671(e)(4); stipulating that net heating value (NHV) calculations must use individual component properties in Table 12 to 40 CFR part 63, subpart CC in 63.671(e)(4)(ii); removing “without the use of gas chromatography” in 40 CFR 63.671(f); adding specificity on using low, mid, and high-level calibration gas cylinders in 40 CFR 63.671(f)(2); and revising the calibration requirements for “net heating value by mass spectrometer” in Table 13 to 40 CFR part 63, subpart CC.

Response: First, we noted that there was no difference between the regulatory language from the commenter and the proposed rule revisions for 40 CFR 63.671(e), therefore no changes were considered for this provision.

Next, we considered the commenter recommended revisions to 40 CFR 63.671(e)(4). It appears this suggested revision is intended to clarify that consistent with Performance Specification 9, an initial calibration error test must occur over a 7-day period followed by daily calibration with mid-level calibration standard for each analyte and quarterly performance audits. We have finalized clarifying language in 40 CFR 63.671(e)(4) consistent with our understanding of the commenter’s intent as follows, “The owner or operator must initially determine the average instrument calibration error during the 7-Day Calibration Error Test Period and subsequently perform daily calibration and quarterly audits using either the compound-specific calibration error method provided in paragraph (i) of this section or using the NHV method provided in paragraph (ii) of this section.”

The commenter also suggested a clarifying edit to the definition of equation term “NHV measured” to specify that NHV calculations are to be made based on the individual component properties listed in Table 12. We find that the suggested edit

improves clarity that the individual components and respective properties are contained in Table 12 to 40 CFR part 63, subpart CC, and have finalized this edit consistent with the commenter’s suggestion.

We are not finalizing any amendments to the proposed new introductory paragraph in 40 CFR 63.671(f) as per the commenter’s recommendation to strike “without the use of gas chromatography.” This language provides the clarification that the provisions in 40 CFR 63.671(f) are limited in applicability to continuous mass spectrometers that do not use gas chromatography. We are, however, finalizing the commenter’s recommended revision to 40 CFR 63.671(f)(2) to add the characterizing language (*i.e.*, low-, mid-, high-) relative to the calibration gas cylinders as this language is consistent with Performance Specification 9 specific in sections 7.1.1–7.1.3.

Finally, we are finalizing the proposed amendments to Table 13 to 40 CFR part 63, subpart CC, as proposed, by cross referencing Performance Specification 9 rather than referring to the requirements in 40 CFR 63.671(e)(4) and (f). Performance Specification 9 includes additional requirements than are listed in 40 CFR 63.671(e)(4) and (f). For example, in section 10.2 of Performance Specification 9, if the instrument average response varies by more than 10 percent of the certified concentration value of the cylinder for an analyte, the owner or operator must immediately inspect the instrument making any necessary adjustments and conduct an initial multi-point calibration in accordance with section 10.1. We intended for affected sources to comply fully with the calibration and quality control requirements in Performance Specification 9 and thus are maintaining the cross reference in Table 13 to 40 CFR part 63, subpart CC.

Topic summary, Alternate Test Method for flare fuel measurements (40 CFR 63.671(e)): The EPA approved an Alternate Test Method to use NHV in place of component heat content (*i.e.*, British thermal units “BTU”) for select quality control criteria in 40 CFR part 63, subpart CC flare fuel measurements (herein referred to as ALT–131) in December 2018. See 84 FR 7363, 7364 (March 4, 2019).

Comment: The commenter requested that the EPA clarify whether the ability to use this approved Alternate Method 131 is affected by this rulemaking.

Response: We confirm that the approval of ALT–131 will be unaffected by this rulemaking and facilities can continue to utilize ALT–131 for

compliance with flare measurement requirements in 40 CFR 63.671(e) and by reference, 40 CFR part 60, appendix B, Performance Specification 9 (PS 9) for determining NHV.

Topic summary, LEL clarification (40 CFR 63.643(c), 63.655(g)(13), 63.655(i)(12)): Maintenance vent provisions reference the term LEL to determine compliance. We did not propose revisions to this term but commenters provided feedback stating it was being misused.

Comments: Commenters stated that we were misusing the term LEL in certain rule language provisions for maintenance vents (*e.g.*, 40 CFR 63.643(c)(1)). Commenters stated the LEL was a fixed physical property of a vapor mixture and thus does not change nor is it measured. It refers to a specific concentration value for a particular mixture. For example, when opening a maintenance vent, commenters elaborated that you measure the concentration of the vapor and then you can compare that concentration to the LEL. The rule text incorrectly implied that the LEL of the vapor is measured. The commenters requested that the EPA clarify that the concentration of the vapors in equipment for maintenance vents must be less than 10 percent of the LEL and that facilities are to measure the concentration, not the LEL.

Response: We agree with commenters that the rule text referring to the LEL was used incorrectly for certain maintenance vent and storage vessel degassing provisions and that the LEL cannot be changed for a vapor. We are revising the rule text to be clear that facilities measure the vapor concentration and then compare that concentration value to the LEL of the vapor to determine if the concentration is less than 10 percent of the LEL.

G. What compliance dates are we finalizing?

We are finalizing new compliance dates for certain revisions to the EMACT standards, OLD NESHAP, MON, and Petroleum Refinery MACT 1. We did not propose new compliance dates for the EMACT standards, OLD NESHAP, and MON because the rules that were promulgated in 2020 had still not come into full effect at the time of proposal in April 2023. The compliance dates were also not stayed as part of this reconsideration action. The compliance dates for the 2020 rules have now passed and owners and operators must have been complying with the EMACT standards by July 6, 2023, the OLD NESHAP by July 7, 2023, and the MON by August 12, 2023. Most of the revisions we are finalizing do not

impose substantial new requirements, but rather either provide clarity to the rules for owners and operators or are alternative requirements. As such, we are providing new compliance dates for the EMACT standards, OLD NESHAP, and MON for revisions related to the removal of the *force majeure* provisions only and are not changing the compliance dates for any other revisions to these rules.

For the removal of the *force majeure* provisions from the PRD and emergency flaring work practice standards for each rule and for most actions that we are finalizing for the Petroleum Refinery MACT 1, we are positing that facilities would need some time to successfully accomplish these revisions, including time to read and understand the amended rule requirements; to evaluate their operations to ensure that they can meet the standards during periods of startup and shutdown, as defined in the rule; and to make any necessary adjustments, including adjusting standard operating procedures and converting reporting mechanisms to install necessary hardware and software. The EPA recognizes the confusion that multiple compliance dates for individual requirements would create and the additional burden such an assortment of dates would impose. From our assessment of the timeframe needed for compliance with the revised requirements, the EPA considers a period of 60 days after the effective date of the final rule to be the most expeditious compliance period practicable. Therefore, for the EMACT Standards, OLD NESHAP, MON, and Petroleum Refinery MACT 1, we are finalizing that the *force majeure* provisions shall be fully removed from the PRD and emergency flaring work practice standards as of 60 days after the effective date of the final rule. For the Petroleum Refinery MACT 1, we are also finalizing that affected sources must be in compliance with most other revisions upon initial startup or within 60 days of the effective date of the final rule, whichever is later.

We are finalizing that petroleum refinery owners or operators may comply with the new operating and monitoring requirements for flares upon initial startup or by the effective date of the final rule, whichever is later. We believe that compliance with the flare requirements immediately upon finalizing the rule is necessary to ensure that pressure-assisted flares are appropriately operated.

IV. Summary of Cost, Environmental and Economic Impacts

A. What are the affected facilities?

In our final RTRs, we estimated the following:

There are 26 facilities subject to the EMACT standards that are currently operating and five additional facilities under construction. A complete list of known facilities in the EMACT standards is available in Appendix A of the memorandum, *Review of the RACT/BACT/LAER Clearinghouse Database for the Ethylene Production Source Category* (see Docket Item No. EPA-HQ-OAR-2017-0357-0008 in the EMACT RTR docket).

There are 173 OLD NESHAP facilities currently operating and four additional OLD NESHAP facilities under construction. A complete list of known OLD NESHAP facilities is available in Appendix A of the memorandum, *National Impacts of the 2020 Risk and Technology Review Final Rule for the Organic Liquids Distribution (Non-Gasoline) Source Category* (see Docket Item No. EPA-HQ-OAR-2018-0746-0069 in the OLD NESHAP RTR docket).

There are 201 MON facilities currently operating. A complete list of known MON facilities is available in Appendix 1 of the memorandum, *Residual Risk Assessment for the Miscellaneous Organic Chemical Manufacturing Source Category in Support of the 2019 Risk and Technology Review Proposed Rule* (see Docket Item No. EPA-HQ-OAR-2018-0746-0011 in the MON RTR docket).

Additionally, based on the Energy Information Administration's 2021 Refinery Capacity Report, there are 129 operable petroleum refineries in the United States (U.S.) and the U.S. territories, all of which are expected to be major sources of HAP emissions.

B. What are the air quality impacts?

We did not estimate baseline emissions or emissions reductions for the revisions. None of the revisions have a direct and quantifiable impact on emissions because they are minor revisions to existing requirements.

C. What are the cost impacts?

We expect minimal to no cost impacts due to the revisions. There could be minor costs for affected facilities related to reading the rule, making minor updates to operating procedures in some limited cases, and making minor adjustments to reporting systems. A few revisions provide slightly greater flexibility and could yield minor cost savings. Any potential costs or cost savings are expected to be negligible.

D. What are the economic impacts?

No economic impacts are anticipated due to the revisions because any potential cost impacts are expected to be very minor.

E. What are the benefits?

The proposed revisions are not expected to yield air quality benefits because emissions will not be affected. However, the revisions should improve clarity, monitoring, compliance, and implementation of the rules for the affected source categories.

F. What analysis of environmental justice did we conduct?

The revisions are not expected to impact emissions and therefore we did not conduct an environmental justice analysis. However, environmental justice analyses were conducted for the final 2020 rules for the EMACT standards, OLD NESHAP, and MON.³⁴

V. Statutory and Executive Order Reviews

Additional information about these statutes and Executive orders can be found at <https://www.epa.gov/laws-regulations/laws-and-executive-orders>.

A. Executive Order 12866: Regulatory Planning and Review and Executive Order 14094: Modernizing Regulatory Review

This action is not a significant regulatory action as defined in Executive Order 12866, as amended by Executive Order 14094, and was therefore not subject to a requirement for Executive Order 12866 review.

B. Paperwork Reduction Act (PRA)

This action does not impose any new information collection burden under the PRA for the EMACT standards, OLD NESHAP, MON, or the Petroleum Refinery MACT 1. We finalized certain technical revisions, including new electronic reporting provisions for the PRD and emergency flaring work practice standard, but the technical revisions do not result in changes to the information collection burden. The final amendments require facilities to submit the work practice related data using an EPA provided spreadsheet template electronically through CDX using CEDRI. These data would not be expected to also be included in a facility's submission to the delegated State authority and/or EPA Regional Office such that no duplication is expected. The amendments to the mode of reporting of the work practice

³⁴ 85 FR 40415 (Jul. 6, 2020); 85 FR 40757 (Jul. 7, 2020); and 85 FR 49129 (Aug. 12, 2020).

standard-related data are not expected to change the current burden under the PRA and we did not revise the information collection request (ICR) for the rules. The Office of Management and Budget (OMB) has previously approved the information collection activities contained in the existing regulations at 40 CFR part 63, subpart YY and has assigned OMB control number 2060–0489; 40 CFR part 63, subpart EEEE and has assigned OMB control number 2060–0539; 40 CFR part 63, subpart FFFF and has assigned OMB control number 2060–0533; and 40 CFR part 63, subpart CC and has assigned OMB control number 2060–0340.

C. Regulatory Flexibility Act (RFA)

I certify that this action will not have a significant economic impact on a substantial number of small entities under the RFA. The small entities subject to the requirements of this action are already identified in the 2020 final rules for the EMAX standards, OLD NESHAP, MON, and the 2015 final rule for Petroleum Refineries. The amendments to 40 CFR part 63, subparts CC, YY, EEEE, and FFFF would only minimally change the existing requirements for all entities. There could be minor costs for affected facilities related to reading the final rule, making minor updates to operating procedures in some limited cases, and making minor adjustments to reporting systems. A few revisions provide slightly greater flexibility and could yield minor cost savings. Any potential costs or cost savings are negligible.

D. Unfunded Mandates Reform Act (UMRA)

This action does not contain an unfunded mandate of \$100 million or more as described in UMRA, 2 U.S.C. 1531–1538, and does not significantly or uniquely affect small governments. While this action creates an enforceable duty on the private sector, the annual cost does not exceed \$100 million or more.

E. Executive Order 13132: Federalism

This action does not have federalism implications. It will not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government.

F. Executive Order 13175: Consultation and Coordination With Indian Tribal Governments

This action does not have Tribal implications as specified in Executive

Order 13175. It will not have substantial new direct effects on Tribal governments, on the relationship between the Federal Government and Indian Tribes, or on the distribution of power and responsibilities between the Federal Government and Indian Tribes, as specified in Executive Order 13175. Thus, Executive Order 13175 does not apply to this action.

G. Executive Order 13045: Protection of Children From Environmental Health Risks and Safety Risks

Executive Order 13045 directs federal agencies to include an evaluation of the health and safety effects of the planned regulation on children in Federal health and safety standards and explain why the regulation is preferable to potentially effective and reasonably feasible alternatives. This action is not subject to Executive Order 13045 because it is not a significant regulatory action under section 3(f)(1) of Executive Order 12866, and because the EPA does not believe the environmental health or safety risks addressed by this action present a disproportionate risk to children.

H. Executive Order 13211: Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution, or Use

This action is not subject to Executive Order 13211, because it is not a significant regulatory action under Executive Order 12866.

I. National Technology Transfer and Advancement Act (NTTAA) and 1 CFR Part 51

This rulemaking involves technical standards. The EPA has decided to use Methods 1, 1A, 2, 2A, 2C, 2D, 2F, 2G, 3B, 4, 5, 18, 21, 22, 25, 25A, 27, and 29 of 40 CFR part 60, appendix A; 301, 316, and 320 of 40 CFR part 63, appendix A; and 602 and 624 of 40 CFR part 136, appendix A.

While the EPA identified candidate VCS as being potentially applicable, the Agency decided not to use the VCS identified. The use of voluntary consensus standards for measuring emissions of pollutants or their surrogates subject to emission standards in the rule would not be practical due to lack of equivalency, documentation, validation data and other important technical and policy considerations. Additional information for the VCS search and determinations can be found in the memorandum, *Voluntary Consensus Standard Results for National Emission Standards for Hazardous Air Pollutants: for Ethylene Production, Miscellaneous Organic*

Chemical Manufacturing, Organic Liquids Distribution (Non-Gasoline), and Petroleum Refineries, which is available in the docket for this action.

The following standards appear in the amendatory text of this document and were previously approved for the locations in which they appear: SW–846–5031, SW–846–8260D, and SW–846–5030B.

J. Executive Order 12898: Federal Actions To Address Environmental Justice in Minority Populations and Low-Income Populations and Executive Order 14096: Revitalizing Our Nation's Commitment to Environmental Justice for All

The EPA believes that this type of action does not concern human health or environmental conditions and therefore cannot be evaluated with respect to potentially disproportionate and adverse effects on communities with environmental justice concerns. As discussed in section IV.F. of this preamble, the revisions are not expected to impact emissions, and thus, no changes to human health or environmental conditions are expected.

Although this action does not concern human health or environmental conditions, the EPA identified and addressed environmental justice concerns when conducting analyses for the final 2020 rules for the EMAX standards, OLD NESHAP, and MON. Further information regarding these environmental justice analyses is available at 85 FR 40415 (July 6, 2020), 85 FR 40757 (July 7, 2020), and 85 FR 49129 (August 12, 2020), respectively.

K. Congressional Review Act (CRA)

This action is subject to the CRA, and the EPA will submit a rule report to each House of the Congress and to the Comptroller General of the United States. This action is not a “major rule” as defined by 5 U.S.C. 804(2).

List of Subjects in 40 CFR Part 63

Environmental protection, Air pollution control, Hazardous substances, Incorporation by reference, Reporting and recordkeeping requirements.

Michael S. Regan,
Administrator.

For the reasons stated in the preamble, the Environmental Protection Agency amends part 63 of title 40, chapter I, of the Code of Federal Regulations as follows:

PART 63—NATIONAL EMISSION STANDARDS FOR HAZARDOUS AIR POLLUTANTS FOR SOURCE CATEGORIES

■ 1. The authority citation for part 63 continues to read as follows:

Authority: 42 U.S.C. 7401 *et seq.*

Subpart CC—National Emission Standards for Hazardous Air Pollutants From Petroleum Refineries

■ 2. Amend § 63.641 by revising the entry “Flare” to read as follows:

§ 63.641 Definitions.

* * * * *
Flare means a combustion device lacking an enclosed combustion chamber that uses an uncontrolled volume of ambient air to burn gases. For the purposes of this rule, the definition of flare includes, but is not necessarily limited to, pressure-assisted flares, air-assisted flares, steam-assisted flares, and non-assisted flares.
* * * * *

■ 3. Amend § 63.643 by revising and republishing paragraphs (c)(1) and (2) to read as follows:

§ 63.643 Miscellaneous process vent provisions.

* * * * *
(c) * * *
(1) Prior to venting to the atmosphere, process liquids are removed from the equipment as much as practical and the equipment is depressured to a control device meeting requirements in paragraphs (a)(1) or (2) of this section, a fuel gas system, or back to the process until one of the following conditions, as applicable, is met.

(i) The concentration of the vapor in the equipment served by the maintenance vent is less than 10 percent of its lower explosive limit (LEL).

(ii) If there is no ability to measure the concentration of the vapor in the equipment based on the design of the equipment, the pressure in the equipment served by the maintenance vent is reduced to 5 pounds per square inch gauge (psig) or less. Upon opening the maintenance vent, active purging of the equipment cannot be used until the concentration of the vapors in the maintenance vent (or inside the equipment if the maintenance is a hatch or similar type of opening) is less than 10 percent of its LEL.

(iii) The equipment served by the maintenance vent contains less than 72 pounds of total volatile organic compounds (VOC).

(iv) If the maintenance vent is associated with equipment containing

pyrophoric catalyst (e.g., hydrotreaters and hydrocrackers) and a pure hydrogen supply is not available at the equipment at the time of the startup, shutdown, maintenance, or inspection activity, the concentration of the vapor in the equipment must be less than 20 percent of its LEL, except for one event per year not to exceed 35 percent of its LEL.

(v) If, after applying best practices to isolate and purge equipment served by a maintenance vent, none of the applicable criterion in paragraphs (c)(1)(i) through (iv) of this section can be met prior to installing or removing a blind flange or similar equipment blind, the pressure in the equipment served by the maintenance vent is reduced to 2 psig or less. Active purging of the equipment may be used provided the equipment pressure at the location where purge gas is introduced remains at 2 psig or less.

(2) Except for maintenance vents complying with the alternative in paragraph (c)(1)(iii) of this section, the owner or operator must determine the concentration of the vapor or, if applicable, equipment pressure using process instrumentation or portable measurement devices and follow procedures for calibration and maintenance according to manufacturer’s specifications.
* * * * *

■ 4. Amend § 63.648 by revising paragraphs (j)(3)(iv), (j)(3)(v)(B) and (C), (j)(6) introductory text, and (j)(6)(ii) to read as follows:

§ 63.648 Equipment leak standards.

* * * * *
(j) * * *
(3) * * *
(iv) The owner or operator shall determine the total number of release events that occurred during the calendar year for each affected pressure relief device separately. Prior to June 3, 2024, the owner or operator shall also determine the total number of release events for each pressure relief device for which the root cause analysis concluded that the root cause was a force majeure event, as defined in this subpart.

(v) * * *
(B) Prior to June 3, 2024, a second release event not including force majeure events from a single pressure relief device in a 3 calendar year period for the same root cause for the same equipment. On and after June 3, 2024, a second release event from a single pressure relief device in a 3 calendar year period for the same root cause for the same equipment.

(C) Prior to June 3, 2024, a third release event not including force

majeure events from a single pressure relief device in a 3 calendar year period for any reason. On and after June 3, 2024, a third release event from a single pressure relief device in a 3 calendar year period for any reason.

* * * * *
(6) *Root cause analysis and corrective action analysis.* A root cause analysis and corrective action analysis must be completed as soon as possible, but no later than 45 days after a release event. Special circumstances affecting the number of root cause analyses and/or corrective action analyses are provided in paragraphs (j)(6)(i) through (iii) of this section.
* * * * *

(ii) Prior to June 3, 2024, you may conduct a single root cause analysis and corrective action analysis for a single emergency event that causes two or more pressure relief devices to release, regardless of the equipment served, if the root cause is reasonably expected to be a force majeure event, as defined in this subpart.
* * * * *

■ 5. Amend § 63.655 by:
■ a. Revising paragraphs (g) introductory text, (g)(10) introductory text, (g)(10)(iv), (g)(11) introductory text, (g)(11)(iii) and (iv), and (g)(13)(iii);
■ b. Adding paragraph (i)(9)(vi); and
■ c. Revising paragraphs (i)(11)(ii), (i)(12)(ii), (i)(12)(iii), (i)(12)(v), and (i)(12)(vi).

The addition and revisions read as follows:

§ 63.655 Reporting and recordkeeping requirements.

* * * * *
(g) The owner or operator of a source subject to this subpart shall submit Periodic Reports no later than 60 days after the end of each 6-month period when any of the information specified in paragraphs (g)(1) through (7) of this section or paragraphs (g)(9) through (14) of this section is collected. The first 6-month period shall begin on the date the Notification of Compliance Status report is required to be submitted. A Periodic Report is not required if none of the events identified in paragraphs (g)(1) through (7) of this section or paragraphs (g)(9) through (14) of this section occurred during the 6-month period unless emissions averaging is utilized. Quarterly reports must be submitted for emission points included in emission averages, as provided in paragraph (g)(8) of this section. An owner or operator may submit reports required by other regulations in place of or as part of the Periodic Report required by this paragraph (g) if the reports contain the

information required by paragraphs (g)(1) through (14) of this section. The Periodic Report must contain company identifier information (including the company name and address), the beginning and ending dates of the time period covered by the report, and the information specified in paragraphs (g)(1) through (14) of this section, and it must be submitted in accordance with § 63.10(a) of this part. On or after April 4, 2024, upon initial startup, or once the form has been available on the CEDRI website for six months, whichever date is later, owners or operators must submit all subsequent Periodic Reports in accordance with § 63.10(a) of this part except for the items in paragraphs (g)(10)(iv) and (11)(iv) of this section. The items in paragraphs (g)(10)(iv) and (11)(iv) of this section must be submitted using the appropriate electronic report template on the CEDRI website (<https://www.epa.gov/electronic-reporting-air-emissions/cedri>) for this subpart and following the procedure specified in § 63.9(k), except any medium submitted through mail must be sent to the attention of the Refinery Sector lead. The date report templates become available will be listed on the CEDRI website. Unless the Administrator or delegated state agency or other authority has approved a different schedule for submission of reports, the report must be submitted by the deadline specified in this subpart, regardless of the method in which the report is submitted.

* * * * *

(10) For pressure relief devices subject to the requirements § 63.648(j), Periodic Reports must include the information specified in paragraphs (g)(10)(i) through (iv) of this section. Owners or operators must submit the Periodic Report in accordance with § 63.10(a) of this part. On or after April 4, 2024 or once the report template for this subpart has been available on the CEDRI website for six months, whichever date is later, owners or operators must submit subsequent Periodic Reports in accordance with § 63.10(a) of this part except for the items in paragraph (iv) of this section. The items in paragraph (iv) of this section must be submitted using the appropriate electronic report template on the CEDRI website for this subpart and following the procedures specified in § 63.9(k), except any medium submitted through mail must be sent to the attention of the Refinery Sector lead. The date report templates become available will be listed on the CEDRI website. Unless the Administrator or delegated state agency or other authority has approved a

different schedule for submission of reports, the report must be submitted by the deadline specified in this subpart, regardless of the method in which the report is submitted.

* * * * *

(iv) For each pressure release to the atmosphere during the reporting period from a pressure relief device in organic HAP service subject to § 63.648(j)(3), report the following information:

(A) Pressure relief device identification name or number.

(B) The start time and date of the pressure release.

(C) The duration of the pressure release (in hours).

(D) An estimate of the mass quantity of each organic HAP released (in pounds).

(E) The results of any root cause analysis and corrective action analysis completed during the reporting period, including the corrective actions implemented during the reporting period and, if applicable, the implementation schedule for planned corrective actions to be implemented subsequent to the reporting period.

(11) For flares subject to § 63.670, Periodic Reports must include the information specified in paragraphs (g)(11)(i) through (iv) of this section. Owners or operators must submit the Periodic Report in accordance with § 63.10(a) of this part. On or after April 4, 2024 or once the report template for this subpart has been available on the CEDRI website for six months, whichever date is later, owners or operators must submit subsequent Periodic Reports in accordance with § 63.10(a) of this part except for the items in paragraph (iv) of this section. The items in paragraph (iv) of this section must be submitted using the appropriate electronic report template on the CEDRI website and following the procedures specified in § 63.9(k), except any medium submitted through mail must be sent to the attention of the Refinery Sector lead. The date report templates become available will be listed on the CEDRI website. Unless the Administrator or delegated State agency or other authority has approved a different schedule for submission of reports, the report must be submitted by the deadline specified in this subpart, regardless of the method in which the report is submitted.

* * * * *

(iii) The 15-minute block periods for which the applicable operating limits specified in § 63.670(d) through (f) are not met. Indicate the date and time for the period, the type of deviation (*e.g.*, flare tip velocity, valve position for

pressure-assisted flares, combustion zone net heating value, or net heating value dilution parameter) and the flare tip velocity, if applicable, and the net heating value operating parameter(s) determined following the methods in § 63.670(k) through (n) as applicable.

(iv) An indication whether there were any flaring events meeting the criteria in § 63.670(o)(3) that occurred during the reporting period. If there were flaring events meeting the criteria in § 63.670(o)(3), report the following information for each such flaring event:

(A) Flare identification name or number.

(B) The type of flaring event.

(C) The start and stop time and date of the flaring event.

(D) The length of time (in minutes) for which emissions were visible from the flare during the event.

(E) The periods of time that the flare tip velocity exceeds the maximum flare tip velocity determined using the methods in § 63.670(d)(2) and the maximum 15-minute block average flare tip velocity recorded during the event.

(F) Results of the root cause and corrective actions analysis completed during the reporting period, including the corrective actions implemented during the reporting period and, if applicable, the implementation schedule for planned corrective actions to be implemented subsequent to the reporting period.

* * * * *

(13) * * *

(iii) The lower explosive limit, vessel pressure, or mass of VOC in the equipment, as applicable, at the start of atmospheric venting. If the 5 psig vessel pressure option in § 63.643(c)(1)(ii) was used and active purging was initiated while the concentration of the vapors was 10 percent or greater of its LEL, also include the concentration of the vapors at the time active purging was initiated.

* * * * *

(i) * * *

(9) * * *

(vi) On and after April 4, 2024, for pressure-assisted flares, retain records of pressure and valve positions as required in § 63.670(d)(3) for a minimum of 2 years, records of when valve position was not correct for measured pressure for 5 years, and records of a cross-light performance demonstration as specified in § 63.670(b)(2) for 5 years.

* * * * *

(11) * * *

(ii) Records of the number of releases during each calendar year and, prior to June 3, 2024, the number of those releases for which the root cause was determined to be a force majeure event.

Keep these records for the current calendar year and the past five calendar years.

* * * * *

(12) * * *

(ii) If complying with the requirements of § 63.643(c)(1)(i) and the concentration of the vapor at the time of the vessel opening exceeds 10 percent of its LEL, identification of the maintenance vent, the process units or equipment associated with the maintenance vent, the date of maintenance vent opening, and the concentration of the vapor at the time of the vessel opening.

(iii) If complying with the requirements of § 63.643(c)(1)(ii) and either the vessel pressure at the time of the vessel opening exceeds 5 psig or the concentration of the vapor at the time of the active purging was initiated exceeds 10 percent of its LEL, identification of the maintenance vent, the process units or equipment associated with the maintenance vent, the date of maintenance vent opening, the pressure of the vessel or equipment at the time of discharge to the atmosphere and, if applicable, the concentration of the vapors in the equipment when active purging was initiated.

* * * * *

(v) If complying with the requirements of § 63.643(c)(1)(iv), identification of the maintenance vent, the process units or equipment associated with the maintenance vent, records documenting the lack of a pure hydrogen supply, the date of maintenance vent opening, and the concentration of the vapors in the equipment at the time of discharge to the atmosphere for each applicable maintenance vent opening.

(vi) If complying with the requirements of § 63.643(c)(1)(v), identification of the maintenance vent, the process units or equipment associated with the maintenance vent, records documenting actions taken to comply with other applicable alternatives and why utilization of this alternative was required, the date of maintenance vent opening, the equipment pressure and concentration of the vapors in the equipment at the time of discharge, an indication of whether active purging was performed and the pressure of the equipment during the installation or removal of the blind if active purging was used, the duration the maintenance vent was open during the blind installation or removal process, and records used to estimate the total quantity of VOC in the equipment at the time the maintenance vent was opened to the atmosphere for

each applicable maintenance vent opening.

■ 6. Amend § 63.670 by:

■ a. Revising paragraphs (b) and (d) introductory text;

■ b. Adding paragraph (d)(3);

■ c. Revising paragraphs (e), (l)(5) introductory text, (o)(4)(iv), (o)(6), and (o)(7)(ii) through (o)(7)(v).

The addition and revisions read as follows:

§ 63.670 Requirements for flare control devices.

* * * * *

(b) *Pilot flame presence.* The owner or operator shall operate each flare with a pilot flame present on an individual burner or stage of burners at all times when regulated material is routed to the flare. Each 15-minute block during which there is at least one minute where no pilot flame on an individual burner or stage of burners is present when regulated material is routed to the flare is a deviation of the standard. Deviations in different 15-minute blocks from the same event are considered separate deviations. The owner or operator shall monitor for the presence of a pilot flame on an individual burner or stage of burners as specified in paragraph (g) of this section. Beginning on April 4, 2024, pressure-assisted flares using stages of burners that cross-light must also comply with paragraphs (b)(1) and (2) of this section.

(1) Each stage of burners that cross-lights in the pressure-assisted flare must have at least two pilots with at least one continuously lit and capable of igniting all regulated material that is routed to that stage of burners.

(2) Unless the owner or operator of a pressure-assisted flare chooses to conduct a cross-light performance demonstration as specified in this paragraph, the owner or operator must ensure that if a stage of burners on the flare uses cross-lighting, that the distance between any two burners in series on that stage is no more than 6 feet when measured from the center of one burner to the next burner. A distance greater than 6 feet between any two burners in series may be used provided the owner or operator complies with the requirements in paragraphs (b)(2)(i) through (iii) of this section.

(i) You must conduct a performance demonstration that confirms the pressure-assisted flare will cross-light a minimum of three burners and the spacing between the burners and location of the pilot flame must be representative of the projected installation.

(ii) The compliance demonstration must be approved by the permitting authority and a copy of this approval must be maintained onsite.

(iii) The compliance demonstration report must include the information in paragraphs (b)(2)(iii)(A) through (K) of this section.

(A) A protocol describing the test methodology used, associated test method QA/QC parameters.

(B) The waste gas composition and NHVcz of the gas tested.

(C) The velocity of the waste gas tested.

(D) The pressure-assisted multi-point flare burner tip pressure.

(E) The time, length, and duration of the test.

(F) Records of whether a successful cross-light was observed over all of the burners and the length of time it took for the burners to cross-light.

(G) Records of maintaining a stable flame after a successful cross-light and the duration for which this was observed.

(H) Records of any smoking events during the cross-light.

(I) Waste gas temperature.

(J) Meteorological conditions (e.g., ambient temperature, barometric pressure, wind speed and direction, and relative humidity) during the demonstration.

(K) An indication whether there were any observed flare flameouts and if so, the number and duration of each flare flameout.

* * * * *

(d) *Flare tip velocity.* Except as provided in paragraph (d)(3) of this section for pressure-assisted flares, for each flare, the owner or operator shall comply with either paragraph (d)(1) or (2) of this section, provided the appropriate monitoring systems are in-place, whenever regulated material is routed to the flare for at least 15-minutes and the flare vent gas flow rate is less than the smokeless design capacity of the flare.

* * * * *

(3) Pressure-assisted flares are not subject to the flare tip velocity limits in either paragraph (d)(1) or (2) of this section. In lieu of the flare tip velocity limits, beginning on April 4, 2024, the owner or operator of a pressure-assisted flare must install and operate pressure monitor(s) on the main flare header, as well as a valve position indicator monitoring system for each staging valve to ensure that the flare operates within the proper range of conditions as specified by the manufacturer. The pressure monitor must meet the requirements in Table 13 of this subpart.

(e) *Combustion zone operating limits.* The owner or operator shall operate the flare to maintain the net heating value of flare combustion zone gas (NHV_{cz}) at or above the applicable limits in paragraphs (e)(1) and (2) of this section determined on a 15-minute block period basis when regulated material is routed to the flare for at least 15-minutes. The owner or operator shall monitor and calculate NHV_{cz} as specified in paragraph (m) of this section.

(1) For all flares other than pressure-assisted flares, 270 British thermal units per standard cubic feet (Btu/scf).

(2) Beginning on April 4, 2024, for each pressure-assisted flare, 800 Btu/scf.

* * * * *

(l) * * *
 (5) When a continuous monitoring system is used as provided in paragraph (j)(1) or (3) of this section and, if applicable, paragraph (j)(4) of this section, the owner or operator of a flare other than a pressure-assisted flare may elect to determine the 15-minute block average NHV_{vg} using either the calculation methods in paragraph (l)(5)(i) of this section or the calculation methods in paragraph (l)(5)(ii) of this section. The owner or operator may choose to comply using the calculation methods in paragraph (l)(5)(i) of this section for some non-pressure-assisted flares at the petroleum refinery and comply using the calculation methods (l)(5)(ii) of this section for other flares. However, for each non-pressure-assisted flare, the owner or operator must elect one calculation method that will apply at all times, and use that method for all continuously monitored flare vent streams associated with that flare. If the owner or operator intends to change the calculation method that applies to a flare, the owner or operator must notify the Administrator 30 days in advance of such a change. For pressure-assisted flares, beginning on April 4, 2024, the owner or operator must use the calculation method in paragraph (l)(5)(ii) of this section.

* * * * *

(o) * * *

(4) * * *

(iv) Prior to June 3, 2024, you may conduct a single root cause analysis and corrective action analysis for a single event that causes two or more flares to have a flow event meeting the criteria in paragraph (o)(3)(i) or (ii) of this section, regardless of the configuration of the flares, if the root cause is reasonably expected to be a force majeure event, as defined in this subpart.

* * * * *

(6) The owner or operator shall determine the total number of events for

which a root cause and corrective action analyses was required during the calendar year for each affected flare separately for events meeting the criteria in paragraph (o)(3)(i) of this section and those meeting the criteria in paragraph (o)(3)(ii) of this section. For the purpose of this requirement, a single root cause analysis conducted for an event that met both of the criteria in paragraphs (o)(3)(i) and (ii) of this section would be counted as an event under each of the separate criteria counts for that flare. Additionally, if a single root cause analysis was conducted for an event that caused multiple flares to meet the criteria in paragraph (o)(3)(i) or (ii) of this section, that event would count as an event for each of the flares for each criteria in paragraph (o)(3) of this section that was met during that event. Prior to June 3, 2024, the owner or operator shall also determine the total number of events for which a root cause and correct action analyses was required and the analyses concluded that the root cause was a force majeure event, as defined in this subpart.

(7) * * *

(ii) Prior to June 3, 2024, two visible emissions exceedance events meeting the criteria in paragraph (o)(3)(i) of this section that were not caused by a force majeure event from a single flare in a 3 calendar year period for the same root cause for the same equipment. On and after June 3, 2024, two visible emissions exceedance events meeting the criteria in paragraph (o)(3)(i) of this section from a single flare in a 3 calendar year period for the same root cause for the same equipment.

(iii) Prior to June 3, 2024, two flare tip velocity exceedance events meeting the criteria in paragraph (o)(3)(ii) of this section that were not caused by a force majeure event from a single flare in a 3 calendar year period for the same root cause for the same equipment. On and after June 3, 2024, two flare tip velocity exceedance events meeting the criteria in paragraph (o)(3)(ii) of this section from a single flare in a 3 calendar year period for the same root cause for the same equipment.

(iv) Prior to June 3, 2024, three visible emissions exceedance events meeting the criteria in paragraph (o)(3)(i) of this section that were not caused by a force majeure event from a single flare in a 3 calendar year period for any reason. On and after June 3, 2024, three visible emissions exceedance events meeting the criteria in paragraph (o)(3)(i) of this section from a single flare in a 3 calendar year period for any reason.

(v) Prior to June 3, 2024, three flare tip velocity exceedance events meeting the criteria in paragraph (o)(3)(ii) of this

section that were not caused by a force majeure event from a single flare in a 3 calendar year period for any reason. On and after June 3, 2024, three flare tip velocity exceedance events meeting the criteria in paragraph (o)(3)(ii) of this section from a single flare in a 3 calendar year period for any reason.

* * * * *

- 7. Amend § 63.671 by:
 - a. Revising paragraph (e) introductory text; and
 - b. Adding paragraphs (e)(4) and (f).

The additions and revision read as follows:

§ 63.671 Requirements for flare monitoring systems.

* * * * *

(e) *Additional requirements for gas chromatographs.* For monitors used to determine compositional analysis for net heating value per § 63.670(j)(1) that include a gas chromatograph, the gas chromatograph must also meet the requirements of paragraphs (e)(1) through (4) of this section.

* * * * *

(4) Beginning on April 4, 2024, the owner or operator must initially determine the average instrument calibration error during the Seven (7)-Day Calibration Error Test Period and subsequently perform daily calibration and quarterly audits using either the compound-specific calibration error (CE) method provided in paragraph (i) of this section or using the net heating value (NHV) method provided in paragraph (ii) of this section.

(i) The average instrument CE for each calibration compound at any calibration concentration must not differ by more than 10 percent from the certified cylinder gas value. The CE for each component in the calibration blend must be calculated using the following equation:

Where:

$$CE = \frac{C_m - C_a}{C_a} \times 100$$

Where:

C_m = Average instrument response (ppm).
 C_a = Certified cylinder gas value (ppm).

(ii) The CE for NHV at any calibration level must not differ by more than 10 percent from the certified cylinder gas value. The CE for must be calculated using the following equation:

$$CE = \frac{NHV_{measured} - NHV_a}{NHV_a} \times 100$$

Where:

NHV_{measured} = Average instrument response (Btu/scf). NHV calculations must be based on the individual component properties in table 12 of this subpart.

NHV_a = Certified cylinder gas value (Btu/scf).

(f) *Additional requirements for continuous process mass spectrometers.* Beginning on April 4, 2024, for continuous process mass spectrometers used to determine compositional analysis for net heating value per § 63.670(j)(1) without the use of gas chromatography, the continuous process mass spectrometer must also meet the requirements of paragraphs (f)(1) through (7) of this section.

(1) You must meet the calibration gas requirements in paragraph (e)(2) of this section. You may augment the minimum list of calibration gas components found in paragraph (e)(2) of this section with compounds found during a pre-survey or known to be in the gas through process knowledge.

(2) Calibration gas cylinders (*i.e.*, low-, mid-, and high-levels) must be certified to an accuracy of 2 percent and traceable to National Institute of Standards and Technology (NIST) standards.

(3) For unknown gas components that have similar analytical mass fragments to calibration compounds, you may report the unknowns as an increase in the overlapped calibration gas compound. For unknown compounds that produce mass fragments that do not overlap calibration compounds, you may use the response factor for the nearest molecular weight hydrocarbon in the calibration mix to quantify the unknown component's net heating value of flare vent gas (NHV_{vg}).

(4) You may use the response factor for n-pentane to quantify any unknown

components detected with a higher molecular weight than n-pentane.

(5) You must perform an initial calibration to identify mass fragment overlap and response factors for the target compounds.

(6) You must meet applicable requirements in Table 13 of this subpart for Net Heating Value by Mass Spectrometer.

(7) The owner or operator must estimate the instrument calibration error in accordance with paragraph (e)(4) of this section.

■ 8. Amend appendix to subpart CC of part 63 by revising table 13 to read as follows:

**Appendix to Subpart CC of Part 63—
Tables**

* * * * *

TABLE 13—CALIBRATION AND QUALITY CONTROL REQUIREMENTS FOR CPMS

Parameter	Minimum accuracy requirements	Calibration requirements
Temperature	±1 percent over the normal range of temperature measured, expressed in degrees Celsius (C), or 2.8 degrees C, whichever is greater.	Conduct calibration checks at least annually; conduct calibration checks following any period of more than 24 hours throughout which the temperature exceeded the manufacturer's specified maximum rated temperature or install a new temperature sensor. At least quarterly, inspect all components for integrity and all electrical connections for continuity, oxidation, and galvanic corrosion, unless the CPMS has a redundant temperature sensor. Record the results of each calibration check and inspection. Locate the temperature sensor in a position that provides a representative temperature; shield the temperature sensor system from electromagnetic interference and chemical contaminants.
Flow Rate for All Flows Other Than Flare Vent Gas.	±5 percent over the normal range of flow measured or 1.9 liters per minute (0.5 gallons per minute), whichever is greater, for liquid flow. ±5 percent over the normal range of flow measured or 280 liters per minute (10 cubic feet per minute), whichever is greater, for gas flow. ±5 percent over the normal range measured for mass flow.	Conduct a flow sensor calibration check at least biennially (every two years); conduct a calibration check following any period of more than 24 hours throughout which the flow rate exceeded the manufacturer's specified maximum rated flow rate or install a new flow sensor. At least quarterly, inspect all components for leakage, unless the CPMS has a redundant flow sensor. Record the results of each calibration check and inspection. Locate the flow sensor(s) and other necessary equipment (such as straightening vanes) in a position that provides representative flow; reduce swirling flow or abnormal velocity distributions due to upstream and downstream disturbances.
Flare Vent Gas Flow Rate ...	±20 percent of flow rate at velocities ranging from 0.03 to 0.3 meters per second (0.1 to 1 feet per second). ±5 percent of flow rate at velocities greater than 0.3 meters per second (1 feet per second).	Conduct a flow sensor calibration check at least biennially (every two years); conduct a calibration check following any period of more than 24 hours throughout which the flow rate exceeded the manufacturer's specified maximum rated flow rate or install a new flow sensor. At least quarterly, inspect all components for leakage, unless the CPMS has a redundant flow sensor. Record the results of each calibration check and inspection. Locate the flow sensor(s) and other necessary equipment (such as straightening vanes) in a position that provides representative flow; reduce swirling flow or abnormal velocity distributions due to upstream and downstream disturbances.

TABLE 13—CALIBRATION AND QUALITY CONTROL REQUIREMENTS FOR CPMS—Continued

Parameter	Minimum accuracy requirements	Calibration requirements
Pressure	± 5 percent over the normal operating range or 0.12 kilopascals (0.5 inches of water column), whichever is greater.	<p>Review pressure sensor readings at least once a week for straightline (unchanging) pressure and perform corrective action to ensure proper pressure sensor operation if blockage is indicated.</p> <p>Using an instrument recommended by the sensor's manufacturer, check gauge calibration and transducer calibration annually; conduct calibration checks following any period of more than 24 hours throughout which the pressure exceeded the manufacturer's specified maximum rated pressure or install a new pressure sensor.</p> <p>At least quarterly, inspect all components for integrity, all electrical connections for continuity, and all mechanical connections for leakage, unless the CPMS has a redundant pressure sensor.</p> <p>Record the results of each calibration check and inspection.</p> <p>Locate the pressure sensor(s) in a position that provides a representative measurement of the pressure and minimizes or eliminates pulsating pressure, vibration, and internal and external corrosion.</p>
Net Heating Value by Calorimeter.	± 2 percent of span	<p>Specify calibration requirements in your site specific CPMS monitoring plan. Calibration requirements should follow manufacturer's recommendations at a minimum.</p> <p>Temperature control (heated and/or cooled as necessary) the sampling system to ensure proper year-round operation.</p> <p>Where feasible, select a sampling location at least two equivalent diameters downstream from and 0.5 equivalent diameters upstream from the nearest disturbance. Select the sampling location at least two equivalent duct diameters from the nearest control device, point of pollutant generation, air in-leakages, or other point at which a change in the pollutant concentration or emission rate occurs.</p>
Net Heating Value by Gas Chromatograph.	As specified in Performance Specification 9 of 40 CFR part 60, appendix B.	Follow the procedure in Performance Specification 9 of 40 CFR part 60, appendix B, except that a single daily mid-level calibration check can be used (rather than triplicate analysis), the multi-point calibration can be conducted quarterly (rather than monthly), and the sampling line temperature must be maintained at a minimum temperature of 60 °C (rather than 120 °C).
Net Heating Value by Mass Spectrometer.	As specified in Performance Specifications 9 of 40 CFR part 60, appendix B.	Follow the procedure in Performance Specification 9 of 40 CFR part 60, appendix B, including performing an initial multi-point calibration check at three concentrations following the procedure in section 10.1 of Performance Specification 9, except that the multi-point calibration can be conducted quarterly (rather than monthly), and the sampling line temperature must be maintained at a minimum temperature of 60 °C (rather than 120 °C).
Hydrogen analyzer	± 2 percent over the concentration measured or 0.1 volume percent, whichever is greater.	<p>Specify calibration requirements in your site specific CPMS monitoring plan. Calibration requirements should follow manufacturer's recommendations at a minimum.</p> <p>Where feasible, select the sampling location at least two equivalent duct diameters from the nearest control device, point of pollutant generation, air in-leakages, or other point at which a change in the pollutant concentration occurs.</p>

Subpart YY—National Emission Standards for Hazardous Air Pollutants Air Pollutants for Source Categories: Generic Maximum Achievable Control Technology Standards

■ 9. Amend § 63.1100 by revising paragraphs (b) and (g)(7)(iii) to read as follows:

§ 63.1100 Applicability.

(b) *Subpart A requirements.* The following provisions of subpart A of this part (General Provisions), §§ 63.1 through 63.5, and §§ 63.12 through 63.15, apply to owners or operators of affected sources subject to this subpart. For sources that reclassify from major source to area source status, the applicable provisions of § 63.9(j) and (k) apply. Beginning no later than the compliance dates specified in § 63.1102(c), for ethylene production affected sources, §§ 63.7(a)(4), (c), (e)(4), and (g)(2), § 63.9(k), and 63.10(b)(2)(vi) also apply.

(g) * * *
(7) * * *

(iii) Beginning no later than the compliance dates specified in § 63.1102(c), flares subject to the requirements in 40 CFR part 63, subpart CC and used as a control device for an emission point subject to the requirements in Table 7 to § 63.1103(e) are only required to comply with the flare requirements in 40 CFR part 63, subpart CC.

■ 10. Amend § 63.1102 by revising paragraphs (c)(11), (d)(2)(ii), and (e)(2)(iii) to read as follows:

§ 63.1102 Compliance schedule.

(c) * * *

(11) The requirements in § 63.1108(a)(4), (b)(1)(ii), (b)(2), and (b)(4)(ii)(B).

(d) * * *
(2) * * *

(ii) The compliance requirements specified in § 63.1108(a)(4), (b)(1)(ii), (b)(2), and (b)(4)(ii)(B).

(e) * * *
(2) * * *

(iii) The compliance requirements specified in § 63.1108(a)(4), (b)(1)(ii), (b)(2), and (b)(4)(ii)(B).

■ 11. Amend § 63.1103 by:

■ a. Revising paragraphs (e)(4)(iii), (e)(4)(vii)(B), (e)(5)(i)(A), (e)(5)(i)(B), (e)(5)(ii), and (e)(7)(i);

■ b. Removing paragraphs (e)(7)(i)(A) and (e)(7)(i)(B);

■ c. Revising paragraphs (e)(8)(i) and (e)(10) introductory text; and
■ d. Adding paragraph (e)(10)(iv).

The addition and revisions read as follows:

§ 63.1103 Source category-specific applicability, definitions, and requirements.

(e) * * *
(4) * * *

(iii) Instead of complying with § 63.670(o)(2)(iii) of subpart CC, if required to develop a flare management plan and submit it to the Administrator, then the owner or operator must also submit all versions of the plan in portable document format (PDF) to the EPA following the procedure specified in § 63.9(k), except any medium submitted through U.S. mail must be sent to the attention of the Ethylene Production Sector Lead.

(vii) * * *

(B) The owner or operator must comply with the NHVcz requirements in § 63.670(e)(2) of subpart CC;

(5) * * *
(i) * * *

(A) The concentration of the vapor in the equipment served by the maintenance vent is less than 10 percent of its lower explosive limit (LEL).

(B) If there is no ability to measure the concentration of the vapor in the equipment based on the design of the equipment, the pressure in the equipment served by the maintenance vent is reduced to 5 pounds per square inch gauge (psig) or less. Upon opening the maintenance vent, active purging of the equipment cannot be used until the concentration of the vapors in the maintenance vent (or inside the equipment if the maintenance is a hatch or similar type of opening) is less than 10 percent of its LEL.

(ii) Except for maintenance vents complying with the alternative in paragraph (e)(5)(i)(C) of this section, the owner or operator must determine the concentration of the vapor or, if applicable, equipment pressure using process instrumentation or portable measurement devices and follow procedures for calibration and maintenance according to manufacturer's specifications.

(7) * * *

(i) During normal operations, conduct daily inspections of the firebox burners and repair all burners that are impinging on the radiant tube(s) as soon as practical, but not later than 1 calendar

day after the flame impingement is found. The owner or operator may delay burner repair beyond 1 calendar day provided the repair cannot be completed during normal operations, the burner cannot be shutdown without significantly impacting the furnace heat distribution and firing rate, and action is taken to reduce flame impingement as much as possible during continued operation. If a delay of repair is required to fully resolve burner flame impingement, repair must be completed following the next planned decoking operation (and before returning the ethylene cracking furnace back to normal operations) or during the next ethylene cracking furnace complete shutdown (when the ethylene cracking furnace firebox is taken completely offline), whichever is earlier. An inspection may include, but is not limited to: visual inspection of the radiant tube(s) for localized bright spots (this may be confirmed with a temperature gun), use of luminescent powders injected into the burner to illuminate the flame pattern, or identifying continued localized coke buildup that causes short runtimes between decoking cycles. A repair may include, but is not limited to: Taking the burner out of service, replacing the burner, adjusting the alignment of the burner, adjusting burner configuration, making burner air corrections, repairing a malfunction of the fuel liquid removal equipment, or adding insulation around the radiant tube(s).

(8) * * *

(i) Prior to decoking operation, inspect the applicable ethylene cracking furnace isolation valve(s) to confirm that the radiant tube(s) being decoked is completely isolated from the ethylene production process so that no emissions generated from decoking operations are sent to the ethylene production process. If poor isolation is identified, then the owner or operator must rectify the isolation issue prior to continuing decoking operations to prevent leaks into the ethylene production process, unless the owner or operator determines that damage to the radiant tube(s) or ethylene cracking furnace could occur if the repair was attempted prior to completing a decoking operation and/or prior to the ethylene cracking furnace being shut down.

(10) *Storage vessel degassing.*

Beginning no later than the compliance dates specified in § 63.1102(c), for each storage vessel subject to paragraph (b) or (c) of Table 7 to § 63.1103(e), the owner or operator must comply with

paragraphs (e)(10)(i) through (iv) of this section during storage vessel shutdown operations (*i.e.*, emptying and degassing of a storage vessel) until the vapor space concentration in the storage vessel is less than 10 percent of the LEL. The owner or operator must determine the concentration using process instrumentation or portable measurement devices and follow procedures for calibration and maintenance according to manufacturer's specifications.

* * * * *

(iv) For floating roof storage vessels, the storage vessel may be opened to set up equipment (*e.g.*, making connections to a temporary control device) for the shutdown operations but must not be actively degassed during this time period.

* * * * *

■ 12. Amend § 63.1107 by revising paragraphs (h)(3)(iv), (h)(3)(v)(B) and (C), (h)(6) introductory text, and (h)(6)(ii) to read as follows:

§ 63.1107 Equipment leaks.

* * * * *

(h) * * *

(3) * * *

(iv) The owner or operator must determine the total number of release events that occurred during the calendar year for each affected pressure relief device separately. Prior to June 3, 2024, the owner or operator must also determine the total number of release events for each pressure relief device for which the root cause analysis concluded that the root cause was a force majeure event, as defined in § 63.1103(e)(2).

(v) * * *

(B) Prior to June 3, 2024, a second release event not including force majeure events from a single pressure relief device in a 3-calendar year period for the same root cause for the same equipment. On and after June 3, 2024, a second release event from a single pressure relief device in a 3-calendar year period for the same root cause for the same equipment.

(C) Prior to June 3, 2024, a third release event not including force majeure events from a single pressure relief device in a 3-calendar year period for any reason. On and after June 3, 2024, a third release event from a single pressure relief device in a 3-calendar year period for any reason.

* * * * *

(6) *Root cause analysis and corrective action analysis.* A root cause analysis and corrective action analysis must be completed as soon as possible, but no later than 45 days after a release event. Special circumstances affecting the

number of root cause analyses and/or corrective action analyses are provided in paragraphs (h)(6)(i) through (iii) of this section.

* * * * *

(ii) Prior to June 3, 2024, you may conduct a single root cause analysis and corrective action analysis for a single emergency event that causes two or more pressure relief devices to release, regardless of the equipment served, if the root cause is reasonably expected to be a *force majeure* event, as defined in § 63.1103(e)(2).

* * * * *

■ 13. Amend § 63.1109 by revising paragraphs (f)(2), (3), and (5), and (i)(2) to read as follows:

§ 63.1109 Recordkeeping requirements.

* * * * *

(f) * * *

(2) If complying with the requirements of § 63.1103(e)(5)(i)(A) and the concentration of the vapor at the time of the vessel opening exceeds 10 percent of its LEL, records that identify the maintenance vent, the process units or equipment associated with the maintenance vent, the date of maintenance vent opening, and the concentration of the vapor at the time of the vessel opening.

(3) If complying with the requirements of § 63.1103(e)(5)(i)(B) and either the vessel pressure at the time of the vessel opening exceeds 5 psig or the concentration of the vapor at the time of the active purging was initiated exceeds 10 percent of its LEL, records that identify the maintenance vent, the process units or equipment associated with the maintenance vent, the date of maintenance vent opening, the pressure of the vessel or equipment at the time of discharge to the atmosphere and, if applicable, the concentration of the vapors in the equipment when active purging was initiated.

* * * * *

(5) If complying with the requirements of § 63.1103(e)(5)(i)(D), identification of the maintenance vent, the process units or equipment associated with the maintenance vent, records documenting actions taken to comply with other applicable alternatives and why utilization of this alternative was required, the date of maintenance vent opening, the equipment pressure and concentration of the vapors in the equipment at the time of discharge, an indication of whether active purging was performed and the pressure of the equipment during the installation or removal of the blind if active purging was used, the duration the maintenance vent was

open during the blind installation or removal process, and records used to estimate the total quantity of VOC in the equipment at the time the maintenance vent was opened to the atmosphere for each applicable maintenance vent opening.

* * * * *

(i) * * *

(2) Records of the number of releases during each calendar year and, prior to June 3, 2024, the number of those releases for which the root cause was determined to be a force majeure event. Keep these records for the current calendar year and the past five calendar years.

* * * * *

■ 14. Amend § 63.1110 by revising paragraphs (a)(10), (e)(4)(iii), (e)(4)(iv)(A) and (B), (e)(5)(iii), and (e)(8)(iii) to read as follows:

§ 63.1110 Reporting requirements.

(a) * * *

(10)(i) Beginning no later than the compliance dates specified in § 63.1102(c) for ethylene production affected sources, specified in § 63.1102(d) for cyanide chemicals manufacturing affected sources, and specified in § 63.1102(e) for carbon black production affected sources, within 60 days after the date of completing each performance test required by this subpart or applicability assessment required by § 63.1103(f)(3)(iv), the owner or operator must submit the results of the performance test or applicability assessment following the procedures specified in § 63.9(k). Data collected using test methods supported by the EPA's Electronic Reporting Tool (ERT) as listed on the EPA's ERT website (<https://www.epa.gov/electronic-reporting-air-emissions/electronic-reporting-tool-ert>) at the time of the test must be submitted in a file format generated through the use of the EPA's ERT. Alternatively, you may submit an electronic file consistent with the extensible markup language (XML) schema listed on the EPA's ERT website. Data collected using test methods that are not supported by the EPA's ERT as listed on the EPA's ERT website at the time of the test must be included as an attachment in the ERT or alternate electronic file.

(ii) Beginning no later than the compliance dates specified in § 63.1102(c) through (e), the owner or operator must submit all subsequent Notification of Compliance Status reports required under paragraph (a)(4) of this section in portable document format (PDF) format to the EPA

following the procedure specified in § 63.9(k). All subsequent Periodic Reports required under paragraph (a)(5) of this section must be submitted to the EPA via CEDRI using the appropriate electronic report template on the CEDRI website (<https://www.epa.gov/electronic-reporting-air-emissions/cedri>) for this subpart and following the procedure specified in § 63.9(k) beginning no later than the compliance dates specified in § 63.1102(c) through (e) or once the report template has been available on the CEDRI website for 1 year, whichever date is later. The date report templates become available will be listed on the CEDRI website. Unless the Administrator or delegated State agency or other authority has approved a different schedule for submission of reports under § 63.9(i) and § 63.10(a) of subpart A, the report must be submitted by the deadline specified in this subpart, regardless of the method in which the report is submitted. Any medium submitted through mail under § 63.9(k) for a Notification of Compliance Status report or Periodic Report must be sent to the attention of the Ethylene Production Sector Lead, Cyanide Chemicals Manufacturing Sector Lead, or Carbon Black Production Sector Lead, as appropriate.

(iii) Beginning no later than the compliance date specified in § 63.1102(c) or once the report template for this subpart has been available on the CEDRI website for six months, whichever date is later, the items in § 63.1110(e)(4)(iv) and § 63.1110(e)(8)(iii) must be submitted to the EPA via CEDRI as specified in § 63.9(k) using the appropriate electronic report template on the CEDRI website for reporting that information. The report submitted to CEDRI must also contain company identifier information (including the company name and address) and the beginning and ending dates of the time period covered by the report. Once you begin submitting Periodic Reports to CEDRI in accordance with paragraph (a)(10)(ii) of this section, the items in § 63.1110(e)(4)(iv) and § 63.1110(e)(8)(iii) must be included in those Periodic Reports instead of submitting the information using the separate template.

* * * * *
(e) * * *
(4) * * *

(iii) The periods specified in § 63.1109(e)(6). Indicate the date and start time for the period, and the net heating value operating parameter(s) determined following the methods in

§ 63.670(k) through (n) of subpart CC as applicable.

(iv) * * *
(A) Flare identification name or number and the start and stop time and date of the flaring event.

(B) The length of time (in minutes) that emissions were visible from the flare during the event.

* * * * *
(5) * * *

(iii) The LEL, vessel pressure, or mass of VOC in the equipment, as applicable, at the start of atmospheric venting. If the 5 psig vessel pressure option in § 63.1103(e)(5)(i)(B) was used and active purging was initiated while the concentration of the vapor was 10 percent or greater of its LEL, also include the concentration of the vapors at the time active purging was initiated.

* * * * *
(8) * * *

(iii) For pressure relief devices in organic HAP service subject to § 63.1107(h)(3), report each pressure release to the atmosphere, including pressure relief device identification name or number; start date and start time and duration (in hours) of the pressure release; an estimate (in pounds) of the mass quantity of each organic HAP released; the results of any root cause analysis and corrective action analysis completed during the reporting period, including the corrective actions implemented during the reporting period; and, if applicable, the implementation schedule for planned corrective actions to be implemented subsequent to the reporting period.

* * * * *

Subpart EEEE—National Emission Standards for Hazardous Air Pollutants: Organic Liquids Distribution (Non-Gasoline)

- 15. Amend § 63.2346 by:
 - a. Revising paragraph (a)(6) introductory text;
 - b. Adding paragraph (a)(6)(iv); and
 - c. Revising paragraph (e).

The addition and revisions read as follows:

§ 63.2346 What emission limitations, operating limits, and work practice standards must I meet?

(a) * * *
(6) Beginning no later than the compliance dates specified in § 63.2342(e), tank emissions during storage tank shutdown operations (*i.e.*, emptying and degassing of a storage tank) for each storage tank at an affected source storing organic liquids that meets the tank capacity and liquid vapor pressure criteria for control in items 2

through 6 of Table 2 to this subpart, or items 1 through 3 of Table 2b to this subpart, you must comply with paragraphs (a)(6)(i) through (iv) of this section during tank emptying and degassing until the vapor space concentration in the tank is less than 10 percent of the lower explosive limit (LEL). The owner or operator must determine the concentration using process instrumentation or portable measurement devices and follow procedures for calibration and maintenance according to manufacturer's specifications.

* * * * *

(iv) For floating roof storage tanks, the storage tank may be opened to set up equipment (*e.g.*, making connections to a temporary control device) for the shutdown operations but must not be actively degassed during this time period.

* * * * *

(e) *Operating limits.* For each high throughput transfer rack, you must meet each operating limit in Table 3 to this subpart for each control device used to comply with the provisions of this subpart whenever emissions from the loading of organic liquids are routed to the control device. Except as specified in paragraph (k) of this section, for each storage tank and low throughput transfer rack, you must comply with paragraph (l) of this section and the requirements for monitored parameters as specified in subpart SS of this part, for storage tanks and, during the loading of organic liquids, for low throughput transfer racks, respectively. Alternatively, you may comply with the operating limits in table 3 to this subpart.

* * * * *

- 16. Amend § 63.2378 by revising and republishing paragraph (e) to read as follows:

§ 63.2378 How do I demonstrate continuous compliance with the emission limitations, operating limits, and work practice standards?

* * * * *

(e) Beginning no later than the compliance dates specified in § 63.2342(e), paragraphs (b) through (d) of this section no longer apply. Instead, you must be in compliance with each emission limitation, operating limit, and work practice standard specified in paragraph (a) of this section at all times, except during periods of nonoperation of the affected source (or specific portion thereof) resulting in cessation of the emissions to which this subpart applies and must comply with the requirements specified in paragraphs

(e)(1) through (4) of this section, as applicable. Equipment subject to the work practice standards for equipment leak components in Table 4 to this subpart, item 4 are not subject to this paragraph (e).

(1) Except as specified in paragraphs (e)(3) and (4) of this section, the use of a bypass line at any time on a closed vent system to divert a vent stream to the atmosphere or to a control device not meeting the requirements specified in paragraph (a) of this section is an emissions standards deviation.

(2) If you are subject to the bypass monitoring requirements of § 63.983(a)(3), then you must continue to comply with the requirements in § 63.983(a)(3) and the recordkeeping and reporting requirements in § 63.998(d)(1)(ii) and 63.999(c)(2), in addition to § 63.2346(l), the recordkeeping requirements specified in § 63.2390(g), and the reporting requirements specified in § 63.2386(c)(12).

(3) Periods of planned routine maintenance of a control device used to control storage tank breathing loss emissions, during which the control device does not meet the emission limits in Table 2 or 2b to this subpart, must not exceed 240 hours per year. The level of material in the storage tank shall not be increased during periods that the closed-vent system or control device is bypassed to perform planned routine maintenance.

(4) If you elect to route emissions from storage tanks to a fuel gas system or to a process, as allowed by § 63.982(d), to comply with the emission limits in Table 2 or 2b to this subpart, the total aggregate amount of time during which the breathing loss emissions bypass the fuel gas system or process during the calendar year without being routed to a control device, for all reasons (except product changeovers of flexible operation units and periods when a storage tank has been emptied and degassed), must not exceed 240 hours. The level of material in the storage tank shall not be increased during periods that the fuel gas system or process is bypassed.

* * * * *

■ 17. Amend § 63.2382 by revising paragraph (d)(3) to read as follows:

§ 63.2382 What notifications must I submit and when and what information should be submitted?

* * * * *

(d) * * *

(3) *Submitting Notification of Compliance Status.* Beginning no later than the compliance dates specified in § 63.2342(e), you must submit all subsequent Notification of Compliance Status reports in portable document format (PDF) format to the EPA following the procedure specified in § 63.9(k), except any medium submitted through mail must be sent to the attention of the Organic Liquids Distribution Sector Lead.

■ 18. Amend § 63.2386 by:

■ a. Revising paragraphs (f), (g), and (h); and

■ b. Removing paragraphs (i) and (j).

The revisions read as follows:

§ 63.2386 What reports must I submit and when and what information is to be submitted in each?

* * * * *

(f) Beginning no later than the compliance dates specified in § 63.2342(e), you must submit all Compliance reports to the EPA following the procedure specified in § 63.9(k), except any medium submitted through U.S. mail must be sent to the attention of the Organic Liquids Distribution Sector Lead. You must use the appropriate electronic report template on the CEDRI website (<https://www.epa.gov/electronic-reporting-air-emissions/cedri>) for this subpart. The date report templates become available will be listed on the CEDRI website. Unless the Administrator or delegated state agency or other authority has approved a different schedule for submission of reports under §§ 63.9(i) and 63.10(a), the report must be submitted by the deadline specified in this subpart, regardless of the method in which the report is submitted.

(g) Beginning no later than the compliance dates specified in § 63.2342(e), you must start submitting performance test reports in accordance with this paragraph. Unless otherwise specified in this subpart, within 60 days after the date of completing each performance test required by this subpart, you must submit the results of the performance test following the procedures specified in § 63.9(k). Data collected using test methods supported by the EPA's Electronic Reporting Tool

(ERT) as listed on the EPA's ERT website (<https://www.epa.gov/electronic-reporting-air-emissions/electronic-reporting-tool-ert>) at the time of the test must be submitted in a file format generated through the use of the EPA's ERT. Alternatively, you may submit an electronic file consistent with the XML schema listed on the EPA's ERT website. Data collected using test methods that are not supported by the EPA's ERT as listed on the EPA's ERT website at the time of the test must be included as an attachment in the ERT or alternate electronic file.

(h) Beginning no later than the compliance dates specified in § 63.2342(e), you must start submitting performance evaluation reports in accordance with this paragraph. Unless otherwise specified in this subpart, within 60 days after the date of completing each CEMS performance evaluation (as defined in § 63.2) that includes a relative accuracy test audit (RATA), you must submit the results of the performance evaluation following the procedures specified in § 63.9(k). The results of performance evaluations of CEMS measuring RATA pollutants that are supported by the EPA's ERT as listed on the EPA's ERT website at the time of the evaluation must be included as an attachment in the ERT or alternate electronic file.

§ 63.2406 [Amended]

■ 19. Amend § 63.2406 by removing the definition of "Force majeure event".

■ 20. Amend table 12 to subpart EEEE of part 63 by:

■ a. Adding the entry "63.7(a)(4)" in numerical order; and

■ b. Revising the entry "63.9(k)".

The addition and revision read as follows:

Table 12 to Subpart EEEE of Part 63—Applicability of General Provisions to Subpart EEEE

* * * * *

Citation	Subject	Brief description	Applies to subpart EEEE
§ 63.7(a)(4)	Force Majeure—Performance Testing Delay	Requirements to claim a delay in conducting a performance test due to force majeure.	Yes.
§ 63.9(k)	Electronic reporting procedures	Procedure to report electronically for notifications and reports.	Yes.

Subpart FFFF—National Emission Standards for Hazardous Air Pollutants: Miscellaneous Organic Chemical Manufacturing

■ 21. Amend § 63.2450 by revising paragraphs (e)(1), (e)(5)(iv), (e)(5)(viii)(B), (e)(6)(i), (e)(7) introductory text, (v)(1)(i), (v)(1)(ii), and (v)(2) to read as follows:

§ 63.2450 What are my general requirements for complying with this subpart?

(e) * * *
 (1) Except when complying with § 63.2485 or paragraph (e)(7) of this section, if you reduce organic HAP emissions by venting emissions through a closed-vent system to any combination of control devices (except a flare) or recovery devices, you must meet the requirements of paragraph (e)(4) of this section, and the requirements of § 63.982(c) and the requirements referenced therein.

(iv) * * *
 (iv) Instead of complying with paragraph (o)(2)(iii) of § 63.670 of subpart CC, if required to develop a flare management plan and submit it to the Administrator, then you must also submit all versions of the plan in portable document format (PDF) to the EPA following the procedure specified in § 63.9(k), except any medium submitted through mail must be sent to the attention of the Miscellaneous Organic Chemical Manufacturing Sector Lead.

(viii) * * *
 (B) You must comply with the NHVcz requirements in paragraph (e)(2) of § 63.670 of subpart CC;

(6) * * *
 (i) If you are subject to the bypass monitoring requirements of § 63.148(f) of subpart G, then you must continue to comply with the requirements in § 63.148(f) of subpart G and the

recordkeeping and reporting requirements in §§ 63.148(j)(2) and (3) of subpart G, and § 63.148(i)(3) of subpart G, in addition to the applicable requirements specified in § 63.2485(q), the recordkeeping requirements specified in § 63.2525(n), and the reporting requirements specified in § 63.2520(e)(12).

(7) Beginning no later than the compliance dates specified in § 63.2445(g), if you reduce organic HAP emissions by venting emissions through a closed-vent system to an adsorber(s) that cannot be regenerated or a regenerative adsorber(s) that is regenerated offsite, then you must comply with paragraphs (e)(4) and (6) of this section, § 63.2470(c)(3), §§ 63.2520(d)(6) and (e)(13), § 63.2525(o), the requirements in § 63.983 including the requirements referenced therein, and you must install a system of two or more adsorber units in series and comply with the requirements specified in paragraphs (e)(7)(i) through (iii) of this section.

(v) * * *
 (1) * * *
 (i) The vapor in the equipment served by the maintenance vent has a concentration less than 10 percent of its lower explosive limit (LEL) and has an outlet concentration less than or equal to 20 ppmv hydrogen halide and halogen HAP.

(ii) If there is no ability to measure the concentration of the vapor in the equipment based on the design of the equipment, the pressure in the equipment served by the maintenance vent is reduced to 5 pounds per square inch gauge (psig) or less. Upon opening the maintenance vent, active purging of the equipment cannot be used until the concentration of the vapors in the maintenance vent (or inside the equipment if the maintenance is a hatch or similar type of opening) is less than 10 percent of its LEL.

(2) Except for maintenance vents complying with the alternative in paragraph (v)(1)(iii) of this section, you must determine the concentration of the vapor or, if applicable, equipment pressure using process instrumentation or portable measurement devices and follow procedures for calibration and maintenance according to manufacturer's specifications.

■ 22. Amend § 63.2460 by revising paragraph (c)(9) introductory text to read as follows:

§ 63.2460 What requirements must I meet for batch process vents?

(c) * * *
 (9) *Requirements for a biofilter.* If you use a biofilter to meet either the 95-percent reduction requirement or outlet concentration requirement specified in Table 2 to this subpart, you must meet the requirements specified in paragraphs (c)(9)(i) through (iv) of this section.

■ 23. Amend § 63.2470 by revising paragraph (f) introductory text and adding paragraph (f)(4) to read as follows:

§ 63.2470 What requirements must I meet for storage tanks?

(f) *Storage tank degassing.* Beginning no later than the compliance dates specified in § 63.2445(g), for each storage tank subject to item 1 of Table 4 to this subpart, you must comply with paragraphs (f)(1) through (4) of this section during storage tank shutdown operations (*i.e.*, emptying and degassing of a storage tank) until the vapor space concentration in the storage tank is less than 10 percent of the LEL. You must determine the concentration using process instrumentation or portable measurement devices and follow procedures for calibration and maintenance according to manufacturer's specifications.

(4) For floating roof storage tanks, the storage tank may be opened to set up equipment (e.g., making connections to a temporary control device) for the shutdown operations but must not be actively degassed during this time period.

■ 24. Amend § 63.2480 by revising paragraphs (a), (e)(2)(ii), (e)(2)(iii), (e)(3)(iv), (e)(3)(v)(B), (e)(3)(v)(C), (e)(6)(ii), (f)(18)(iii), (f)(18)(vi), (f)(18)(x), and (f)(18)(xiii) to read as follows:

§ 63.2480 What requirements must I meet for equipment leaks?

(a) You must meet each requirement in table 6 to this subpart that applies to your equipment leaks, except as specified in paragraphs (b) through (f) of this section. For each light liquid pump, pressure relief device, and connector in ethylene oxide service as defined in § 63.2550(i), you must also meet the applicable requirements specified in §§ 63.2492 and 63.2493(d) and (e).

* * * * *

(e) * * *
(2) * * *

(ii) If the pressure relief device includes a rupture disk, either comply with the requirements in paragraph (e)(2)(i) of this section (and do not replace the rupture disk) or install a replacement disk as soon as practicable after a pressure release, but no later than 5 calendar days after the pressure release.

(iii) If the pressure relief device consists only of a rupture disk, install a replacement disk as soon as practicable after a pressure release, but no later than 5 calendar days after the pressure release. You must not initiate startup of the equipment served by the rupture disk until the rupture disc is replaced.

(3) * * *

(iv) You must determine the total number of release events that occurred during the calendar year for each affected pressure relief device separately. Prior to June 3, 2024, you must also determine the total number of release events for each pressure relief device for which the root cause analysis concluded that the root cause was a *force majeure* event, as defined in § 63.2550.

(v) * * *

(B) Prior to June 3, 2024, a second release event not including force majeure events from a single pressure relief device in a 3 calendar year period for the same root cause for the same equipment. On and after June 3, 2024, a second release event from a single pressure relief device in a 3 calendar year period for the same root cause for the same equipment.

(C) Prior to June 3, 2024, a third release event not including force majeure events from a single pressure relief device in a 3 calendar year period for any reason. On and after June 3, 2024, a third release event from a single pressure relief device in a 3 calendar year period for any reason.

* * * * *

(6) * * *

(ii) Prior to June 3, 2024, you may conduct a single root cause analysis and corrective action analysis for a single emergency event that causes two or more pressure relief devices to release, regardless of the equipment served, if the root cause is reasonably expected to be a *force majeure* event, as defined in § 63.2550.

* * * * *

(f) * * *
(18) * * *

(iii) In § 63.181(b)(3)(i), replace the reference to § 63.165(a) with § 63.2480(e)(1).

* * * * *

(vi) The information in § 63.165(a) required to be reported under § 63.182(d)(2)(xiv) is now required to be reported under § 63.2520(e)(15)(i) through (iii).

* * * * *

(x) The reference to § 63.1030(c) in § 63.1023(a)(1)(v) no longer applies. Instead comply with the § 63.2480(e)(1) and (2).

* * * * *

(xiii) The information in § 63.1030(b) required to be reported under § 63.1039(b)(4) is now required to be reported under § 63.2520(e)(15)(i) and (ii).

* * * * *

■ 25. Amend § 63.2490 by:
■ a. Revising paragraphs (a), (d) introductory text, and (d)(4)(iii) introductory text; and
■ b. Adding paragraph (e).

The addition and revisions read as follows:

§ 63.2490 What requirements must I meet for heat exchange systems?

(a) You must comply with each requirement in Table 10 to this subpart that applies to your heat exchange systems, except as specified in paragraphs (b) through (e) of this section.

* * * * *

(d) Unless one or more of the conditions specified in § 63.104(a)(1), (2), (5), and (6) or paragraph (e) of this section are met, beginning no later than the compliance dates specified in § 63.2445(g), the requirements of § 63.104 as specified in Table 10 to this

subpart and paragraphs (b) and (c) of this section no longer apply. Instead, you must monitor the cooling water for the presence of total strippable hydrocarbons that indicate a leak according to paragraph (d)(1) of this section, and if you detect a leak, then you must repair it according to paragraphs (d)(2) and (3) of this section, unless repair is delayed according to paragraph (d)(4) of this section. At any time before the compliance dates specified in § 63.2445(g), you may choose to comply with the requirements in this paragraph (d) in lieu of the requirements of § 63.104 as specified in Table 10 to this subpart and paragraphs (b) and (c) of this section. The requirements in this paragraph (d) do not apply to heat exchange systems that have a maximum cooling water flow rate of 10 gallons per minute or less.

* * * * *

(4) * * *

(iii) The delay of repair action level is a total strippable hydrocarbon concentration (as methane) in the stripping gas of 62 ppmv or, for heat exchange systems with a recirculation rate of 10,000 gallons per minute or less, the delay of repair action level is a total hydrocarbon mass emissions rate (as methane) of 1.8 kg/hr. The delay of repair action level is assessed as described in paragraph (d)(4)(iii)(A) or (B) of this section, as applicable.

* * * * *

(e) If 99 percent by weight or more of the organic compounds that could leak into the heat exchange system are water soluble and have a Henry's Law Constant less than 5.0E-6 at 25 degrees Celsius (atmospheres-cubic meters/mol) and none of the conditions specified in § 63.104(a)(1), (2), (5), and (6) are met, beginning no later than the compliance dates specified in § 63.2445(g), you may monitor the cooling water for leaks according to the requirements in § 63.104(b) in lieu of using the Modified El Paso Method. If you detect a leak according to § 63.104(b), then you must repair it according to paragraph (e)(1) of this section, unless repair is delayed according to paragraph (e)(2) of this section.

(1) If a leak is detected using the methods described in paragraph (e) of this section, you must repair the leak as soon as practicable, but no later than 45 days after identifying the leak, except as specified in paragraph (e)(2) of this section. Repair must include re-monitoring at the monitoring location where the leak was identified to verify that the criteria in § 63.104(b)(6) is no longer met. Actions that can be taken to

achieve repair include but are not limited to:

- (i) Physical modifications to the leaking heat exchanger, such as welding the leak or replacing a tube;
- (ii) Blocking the leaking tube within the heat exchanger;
- (iii) Changing the pressure so that water flows into the process fluid;
- (iv) Replacing the heat exchanger or heat exchanger bundle; or
- (v) Isolating, bypassing, or otherwise removing the leaking heat exchanger from service until it is otherwise repaired.

(2) You may delay repair when the conditions in § 63.104(e) are met.

■ 26. Amend § 63.2492 by revising paragraph (b) to read as follows:

§ 63.2492 How do I determine whether my process vent, storage tank, or equipment is in ethylene oxide service?

* * * * *

(b) For storage tanks, you must determine the concentration of ethylene oxide of the fluid stored in the storage tanks by complying with the requirements in paragraph (b)(1) or (2) of this section.

(1) You must measure the concentration of ethylene oxide of the fluid stored in the storage tanks using Method 624.1 of 40 CFR part 136, appendix A, or preparation by Method 5031 and analysis by Method 8260D (both incorporated by reference, see § 63.14) in the SW-846 Compendium. In lieu of preparation by SW-846 Method 5031, you may use SW-846 Method 5030B (incorporated by reference, see § 63.14), as long as: You do not use a preservative in the collected sample; you store the sample with minimal headspace as cold as possible and at least below 4 degrees C; and you analyze the sample as soon as possible, but in no case longer than 7 days from the time the sample was collected. If you are collecting a sample from a pressure vessel, you must maintain the sample under pressure both during and following sampling.

(2) Unless specified by the Administrator, you may calculate the concentration of ethylene oxide of the fluid stored in the storage tanks if information specific to the fluid stored is available. Information specific to the fluid stored includes concentration data from safety data sheets.

* * * * *

■ 27. Amend § 63.2493 by revising paragraphs (a)(2)(vi) introductory text, (a)(2)(vi)(C), (a)(2)(viii), (b)(2), (b)(4) introductory text, (b)(4)(iv), (b)(6), (d)(1)(iii), (d)(2)(iii), (d)(3), (d)(4)(v), and (e) introductory text to read as follows:

§ 63.2493 What requirements must I meet for process vents, storage tanks, or equipment that are in ethylene oxide service?

* * * * *

(a) * * *

(2) * * *

(vi) If you vent emissions through a closed-vent system to a scrubber with a reactant tank, then you must establish operating parameter limits by monitoring the operating parameters specified in paragraphs (a)(2)(vi)(A) through (C) of this section during the performance test.

* * * * *

(C) Temperature of the scrubber liquid entering the scrubber column. The temperature may be measured at any point after the heat exchanger and prior to entering the top of the scrubber column. Determine the average inlet scrubber liquid temperature as the average of the test run averages.

* * * * *

(viii) If you vent emissions through a closed-vent system to a control device other than a flare, scrubber with a reactant tank, or thermal oxidizer, then you must notify the Administrator of the operating parameters that you plan to monitor during the performance test prior to establishing operating parameter limits for the control device.

* * * * *

(b) * * *

(2) If you choose to reduce emissions of ethylene oxide by venting emissions through a closed-vent system to a non-flare control device that reduces ethylene oxide to less than 1 ppmv as specified in Table 1, 2, or 4 to this subpart, and you choose to comply with paragraph (a)(3)(i) of this section, then continuously monitor the ethylene oxide concentration at the exit of the control device using an FTIR CEMS meeting the requirements of Performance Specification 15 of 40 CFR part 60, appendix B, and § 63.2450(j). If you use an FTIR CEMS, you do not need to conduct the performance testing required in paragraph (b)(3) of this section or the operating parameter monitoring required in paragraphs (b)(4) through (6) of this section.

* * * * *

(4) If you vent emissions through a closed-vent system to a scrubber with a reactant tank, then you must comply with § 63.2450(e)(4) and (6) and the requirements in § 63.983, and you must meet the operating parameter limits specified in paragraphs (b)(4)(i) through (v) of this section.

* * * * *

(iv) Maximum temperature of the scrubber liquid entering the scrubber

column, equal to the average temperature measured during the most recent performance test. Compliance with the inlet scrubber liquid temperature operating limit must be determined continuously on a 1-hour block basis. Use a temperature sensor with a minimum accuracy of ±1 percent over the normal range of the temperature measured, expressed in degrees Celsius, or 2.8 degrees Celsius, whichever is greater.

* * * * *

(6) If you vent emissions through a closed-vent system to a control device other than a flare, scrubber with a reactant tank, or thermal oxidizer, then you must comply with § 63.2450(e)(4) and (6) and the requirements in § 63.983, and you must monitor the operating parameters identified in paragraph (a)(2)(viii) of this section and meet the established operating parameter limits to ensure continuous compliance. The frequency of monitoring and averaging time will be determined based upon the information provided to the Administrator.

* * * * *

(d) * * *

(1) * * *

(iii) When a leak is detected, it must be repaired as soon as practicable, but not later than 15 calendar days after it is detected. Delay of repair of pumps for which leaks have been detected is allowed for pumps that are isolated from the process and that do not remain in ethylene oxide service.

(2) * * *

(iii) When a leak is detected, it must be repaired as soon as practicable, but not later than 15 calendar days after it is detected. Delay of repair of connectors for which leaks have been detected is allowed for connectors that are isolated from the process and that do not remain in ethylene oxide service.

(3) For each light liquid pump or connector in ethylene oxide service that is added to an MCPU, and for each light liquid pump or connector in ethylene oxide service that replaces a light liquid pump or connector in ethylene oxide service, you must initially monitor for leaks within 5 days after initial startup of the equipment.

(4) * * *

(v) Replace all references to § 63.2445(g) with § 63.2445(i).

(e) *Non-applicable referenced provisions.* The referenced provisions specified in paragraphs (e)(1) through (16) of this section do not apply when demonstrating compliance with this section.

* * * * *

■ 28. Amend § 63.2515 by revising paragraph (d) to read as follows:

§ 63.2515 What notifications must I submit and when?

* * * * *

(d) *Supplement to Notification of Compliance Status.* You must also submit supplements to the Notification of Compliance Status as specified in § 63.2520(d)(3) through (6).

■ 29. Amend § 63.2520 by:

■ a. Revising paragraph (d) introductory text;

■ b. Adding paragraph (d)(6);

■ c. Revising paragraphs (e) introductory text, (e)(2), (e)(14)(iii), (e)(16), (f) and (g); and

■ d. Removing paragraphs (h) and (i).

The addition and revisions read as follows:

§ 63.2520 What reports must I submit and when?

* * * * *

(d) *Notification of compliance status report.* You must submit a notification of compliance status report according to the schedule in paragraph (d)(1) of this section, and the notification of compliance status report must contain the information specified in paragraphs (d)(2) through (6) of this section.

* * * * *

(6) For adsorbers subject to the requirements of § 63.2450(e)(7), you must also submit the information listed in paragraphs (d)(6)(i) and (ii) of this section in a supplement to the Notification of Compliance Status within 150 days after the first applicable compliance date.

(i) Whether the adsorber cannot be regenerated or is a regenerative adsorber(s) that is regenerated off site.

(ii) The breakthrough limit and adsorber bed life established during the initial performance test or design evaluation of the adsorber.

(e) *Compliance report.* The compliance report must contain the information specified in paragraphs (e)(1) through (17) of this section. On and after August 12, 2023 or once the reporting template for this subpart has been available on the CEDRI website for 1 year, whichever date is later, you must submit all subsequent reports following the procedure specified in § 63.9(k), except any medium submitted through mail must be sent to the attention of the Miscellaneous Organic Chemical Manufacturing Sector Lead. You must use the appropriate electronic report template on the CEDRI website (<https://www.epa.gov/electronic-reporting-air-emissions/cedri>) for this subpart. The date report templates become available will be listed on the CEDRI website.

Unless the Administrator or delegated state agency or other authority has approved a different schedule for submission of reports under §§ 63.9(i) and 63.10(a) of subpart A, the report must be submitted by the deadline specified in this subpart, regardless of the method in which the report is submitted.

* * * * *

(2) Statement by a responsible official with that official's name, title, and signature, certifying the accuracy of the content of the report. If your report is submitted via CEDRI, the certifier's electronic signature during the submission process replaces the requirement in this paragraph (e)(2).

* * * * *

(14) * * *

(iii) The lower explosive limit in percent, vessel pressure in psig, or mass in pounds of VOC in the equipment, as applicable, at the start of atmospheric venting. If the 5 psig vessel pressure option in § 63.2450(v)(1)(ii) was used and active purging was initiated while the concentration of the vapor was 10 percent or greater of its LEL, also include the concentration of the vapors at the time active purging was initiated.

* * * * *

(16) For each heat exchange system subject to § 63.2490(d) or (e), beginning no later than the compliance dates specified in § 63.2445(g), the reporting requirements of § 63.104(f)(2) no longer apply; instead, the compliance report must include the information specified in paragraphs (e)(16)(i) through (v) of this section.

(i) The number of heat exchange systems at the plant site subject to the monitoring requirements in § 63.2490(d) or (e) during the reporting period;

(ii) The number of heat exchange systems subject to the monitoring requirements in § 63.2490(d) or (e) at the plant site found to be leaking during the reporting period;

(iii) For each monitoring location where a leak was identified during the reporting period, identification of the monitoring location (*e.g.*, unique monitoring location or heat exchange system ID number), the measured total strippable hydrocarbon concentration or total hydrocarbon mass emissions rate (if complying with § 63.2490(d)) or the measured concentration of the monitored substance(s) (if complying with § 63.2490(e)), the date the leak was first identified, and, if applicable, the date the source of the leak was identified;

(iv) For leaks that were repaired during the reporting period (including delayed repairs), identification of the

monitoring location associated with the repaired leak, the total strippable hydrocarbon concentration or total hydrocarbon mass emissions rate (if complying with § 63.2490(d)) or the measured concentration of the monitored substance(s) (if complying with § 63.2490(e)) measured during re-monitoring to verify repair, and the re-monitoring date (*i.e.*, the effective date of repair); and

(v) For each delayed repair, identification of the monitoring location associated with the leak for which repair is delayed, the date when the delay of repair began, the date the repair is expected to be completed (if the leak is not repaired during the reporting period), the total strippable hydrocarbon concentration or total hydrocarbon mass emissions rate (if complying with § 63.2490(d)) or the measured concentration of the monitored substance(s) (if complying with § 63.2490(e)) and date of each monitoring event conducted on the delayed repair during the reporting period, and an estimate in pounds of the potential total hydrocarbon emissions or monitored substance(s) emissions over the reporting period associated with the delayed repair.

* * * * *

(f) *Performance test reports.* Beginning no later than October 13, 2020, you must submit performance test reports in accordance with this paragraph (f). Unless otherwise specified in this subpart, within 60 days after the date of completing each performance test required by this subpart, you must submit the results of the performance test following the procedures specified in § 63.9(k). Data collected using test methods supported by the EPA's Electronic Reporting Tool (ERT) as listed on the EPA's ERT website (<https://www.epa.gov/electronic-reporting-air-emissions/electronic-reporting-tool-ert>) at the time of the test must be submitted in a file format generated through the use of the EPA's ERT. Alternatively, you may submit an electronic file consistent with the extensible markup language (XML) schema listed on the EPA's ERT website. Data collected using test methods that are not supported by the EPA's ERT as listed on the EPA's ERT website at the time of the test must be included as an attachment in the ERT or alternate electronic file.

(g) *CEMS relative accuracy test audit (RATA) Performance evaluation reports.* Beginning no later than October 13, 2020, you must start submitting CEMS RATA performance evaluation reports in accordance with this paragraph (g).

Unless otherwise specified in this subpart, within 60 days after the date of completing each continuous monitoring system performance evaluation (as defined in § 63.2) that includes a RATA, you must submit the results of the performance evaluation following the procedures specified in § 63.9(k). The results of performance evaluations of CEMS measuring RATA pollutants that are supported by the EPA's ERT as listed on the EPA's ERT website at the time of the evaluation must be submitted in a file format generated through the use of the EPA's ERT. Alternatively, you may submit an electronic file consistent with the XML schema listed on the EPA's ERT website. The results of performance evaluations of CEMS measuring RATA pollutants that are not supported by the EPA's ERT as listed on the EPA's ERT website at the time of the evaluation must be included as an attachment in the ERT or alternate electronic file.

■ 30. Amend § 63.2525 by:

■ a. Revising paragraphs (o), (p)(2), (p)(3), (p)(5), (q)(2), (r)(1), (r)(4)(iv) introductory text, (r)(4)(iv)(B) and (r)(4)(iv)(C); and

■ b. Adding paragraph (r)(4)(iv)(D).

The addition and revisions read as follows:

§ 63.2525 What records must I keep?

* * * * *

(o) For each nonregenerative adsorber and regenerative adsorber that is regenerated offsite subject to the requirements in § 63.2450(e)(7), you must keep the applicable records specified in paragraphs (o)(1) through (3) of this section.

(1) Breakthrough limit and bed life established according to § 63.2450(e)(7)(i).

(2) Each outlet HAP or TOC concentration measured according to § 63.2450(e)(7)(ii) and (e)(7)(iii).

(3) Date and time you last replaced the adsorbent.

(p) * * *

(2) If complying with the requirements of § 63.2450(v)(1)(i) and the concentration of the vapor at the time of the vessel opening exceeds 10 percent of its LEL, identification of the maintenance vent, the process units or equipment associated with the maintenance vent, the date of maintenance vent opening, and the concentration of the vapor at the time of the vessel opening.

(3) If complying with the requirements of § 63.2450(v)(1)(ii) and either the vessel pressure at the time of the vessel opening exceeds 5 psig or the concentration of the vapor at the time of the active purging was initiated exceeds

10 percent of its LEL, identification of the maintenance vent, the process units or equipment associated with the maintenance vent, the date of maintenance vent opening, the pressure of the vessel or equipment at the time of discharge to the atmosphere and, if applicable, the concentration of the vapors in the equipment when active purging was initiated.

* * * * *

(5) If complying with the requirements of § 63.2450(v)(1)(iv), identification of the maintenance vent, the process units or equipment associated with the maintenance vent, records documenting actions taken to comply with other applicable alternatives and why utilization of this alternative was required, the date of maintenance vent opening, the equipment pressure and concentration of the vapors in the equipment at the time of discharge, an indication of whether active purging was performed and the pressure of the equipment during the installation or removal of the blind if active purging was used, the duration the maintenance vent was open during the blind installation or removal process, and records used to estimate the total quantity of VOC in the equipment at the time the maintenance vent was opened to the atmosphere for each applicable maintenance vent opening.

(q) * * *

(2) Records of the number of releases during each calendar year and, prior to June 3, 2024, the number of those releases for which the root cause was determined to be a *force majeure* event. Keep these records for the current calendar year and the past 5 calendar years.

* * * * *

(r) * * *

(1) Monitoring data required by § 63.2490(d) and (e) that indicate a leak, the date the leak was detected, or, if applicable, the basis for determining there is no leak.

* * * * *

(4) * * *

(iv) An estimate of the potential total hydrocarbon emissions (if you monitor the cooling water for leaks according to § 63.2490(d)(1)) or monitored substance(s) emissions (if you monitor the cooling water for leaks according to § 63.2490(e)) from the leaking heat exchange system or heat exchanger for each required delay of repair monitoring interval following the procedures in paragraphs (r)(4)(iv)(A) through (D) of this section.

* * * * *

(B) For delay of repair monitoring intervals prior to repair of the leak, calculate the potential total hydrocarbon emissions or monitored substance(s) emissions for the leaking heat exchange system or heat exchanger for the monitoring interval by multiplying the mass emissions rate, determined in § 63.2490(d)(1)(iii)(B) or paragraph (r)(4)(iv)(A) or (D) of this section, by the duration of the delay of repair monitoring interval. The duration of the delay of repair monitoring interval is the time period starting at midnight on the day of the previous monitoring event or at midnight on the day the repair would have had to be completed if the repair had not been delayed, whichever is later, and ending at midnight of the day the of the current monitoring event.

(C) For delay of repair monitoring intervals ending with a repaired leak, calculate the potential total hydrocarbon emissions or monitored substance(s) emissions for the leaking heat exchange system or heat exchanger for the final delay of repair monitoring interval by multiplying the duration of the final delay of repair monitoring interval by the mass emissions rate determined for the last monitoring event prior to the re-monitoring event used to verify the leak was repaired. The duration of the final delay of repair monitoring interval is the time period starting at midnight of the day of the last monitoring event prior to re-monitoring to verify the leak was repaired and ending at the time of the re-monitoring event that verified that the leak was repaired.

(D) If you monitor the cooling water for leaks according to § 63.2490(e), you must calculate the mass emissions rate by determining the mass flow rate of the cooling water at the monitoring location where the leak was detected. Cooling water mass flow rates may be determined using direct measurement, pump curves, heat balance calculations, or other engineering methods. Once determined, multiply the mass flow rate of the cooling water by the concentration of the measured substance(s).

* * * * *

■ 31. Amend § 63.2550 by revising the entry "In ethylene oxide service" to read as follows:

§ 63.2550 What definitions apply to this subpart?

* * * * *

In ethylene oxide service means the following:

(1) For equipment leaks, any equipment that contains or contacts a fluid (liquid or gas) that is at least 0.1 percent by weight of ethylene oxide. If information exists that suggests ethylene

oxide could be present in equipment, the equipment is considered to be “in ethylene oxide service” unless sampling and analysis is performed as specified in § 63.2492 to demonstrate that the equipment does not meet the definition of being “in ethylene oxide service”. Examples of information that could suggest ethylene oxide could be present in equipment, include calculations based on safety data sheets, material balances, process stoichiometry, or previous test results provided the results are still relevant to the current operating conditions.

(2) For process vents, each batch and continuous process vent in a process that, when uncontrolled, contains a concentration of greater than or equal to 1 ppmv undiluted ethylene oxide, and when combined, the sum of all these process vents would emit uncontrolled ethylene oxide emissions greater than or equal to 5 lb/yr (2.27 kg/yr). If information exists that suggests ethylene oxide could be present in a batch or continuous process vent, then the batch or continuous process vent is

considered to be “in ethylene oxide service” unless an analysis is performed as specified in § 63.2492 to demonstrate that the batch or continuous process vent does not meet the definition of being “in ethylene oxide service”. Examples of information that could suggest ethylene oxide could be present in a batch or continuous process vent, include calculations based on safety data sheets, material balances, process stoichiometry, or previous test results provided the results are still relevant to the current operating conditions.

(3) For storage tanks, storage tanks of any capacity and vapor pressure storing a liquid that is at least 0.1 percent by weight of ethylene oxide. If knowledge exists that suggests ethylene oxide could be present in a storage tank, then the storage tank is considered to be “in ethylene oxide service” unless the procedures specified in § 63.2492 are performed to demonstrate that the storage tank does not meet the definition of being “in ethylene oxide service”. The exemptions for “vessels storing organic liquids that contain HAP

only as impurities” and “pressure vessels designed to operate in excess of 204.9 kilopascals and without emissions to the atmosphere” listed in the definition of “storage tank” in this section do not apply for storage tanks that may be in ethylene oxide service. Examples of information that could suggest ethylene oxide could be present in a storage tank, include calculations based on safety data sheets, material balances, process stoichiometry, or previous test results provided the results are still relevant to the current operating conditions.

* * * * *

■ 32. Revise table 10 to subpart FFFF of part 63 to read as follows:

**Table 10 to Subpart FFFF of Part 63—
Work Practice Standards for Heat
Exchange Systems**

As required in § 63.2490, you must meet each requirement in the following table that applies to your heat exchange systems:

For each . . .	You must . . .
Heat exchange system, as defined in § 63.101.	a. Comply with the requirements of § 63.104 and the requirements referenced therein, except as specified in § 63.2490(b) and (c); or b. Comply with the requirements in § 63.2490(d); or c. Comply with the requirements in § 63.2490(e).

■ 33. Amend table 12 to subpart FFFF of part 63 by revising entry “63.9(k)” to read as follows:

**Table 12 to Subpart FFFF of Part 63—
Applicability of General Provisions to
Subpart FFFF**

* * * * *

Citation	Subject	Explanation
§ 63.9(k)	Electronic reporting procedures	Yes.



FEDERAL REGISTER

Vol. 89

Thursday,

No. 66

April 4, 2024

Part V

Department of Commerce

Bureau of Industry and Security

15 CFR Parts 732, 734, 736, et al.

Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections; and Export Controls on Semiconductor Manufacturing Items; Corrections and Clarifications; Interim Final Rule

DEPARTMENT OF COMMERCE**Bureau of Industry and Security**

15 CFR Parts 732, 734, 736, 740, 742, 744, 746, 748, 758, 770, 772, and 774

[Docket No. 240321–0084]

RIN 0694–A194

Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections; and Export Controls on Semiconductor Manufacturing Items; Corrections and Clarifications

AGENCY: Bureau of Industry and Security, Department of Commerce.

ACTION: Interim final rule; request for comments; technical corrections.

SUMMARY: On October 25, 2023, the Bureau of Industry and Security (BIS) published in the **Federal Register** the interim final rules (IFR), “Export Controls on Semiconductor Manufacturing Items” (SME IFR) and “Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections” (AC/S IFR). This rule corrects inadvertent errors in those rules and makes additional clarifications for the two rules.

DATES:

Effective date: This rule is effective April 4, 2024.

Comment due date: Comments for revisions, corrections, and clarifications in this rule must be received by BIS no later than April 29, 2024.

ADDRESSES: Comments on the corrections, revisions, and clarification in this rule may be submitted to the Federal rulemaking portal (www.regulations.gov). The *regulations.gov* ID for this rule is: BIS–2023–0016. Please refer to RIN 0694–AJ23 in all comments.

All filers using the portal should use the name of the person or entity submitting the comments as the name of their files, in accordance with the instructions below. Anyone submitting business confidential information should clearly identify the business confidential portion at the time of submission, file a statement justifying nondisclosure and referring to the specific legal authority claimed, and provide a non-confidential version of the submission.

For comments submitted electronically containing business confidential information, the file name of the business confidential version

should begin with the characters “BC.” Any page containing business confidential information must be clearly marked “BUSINESS CONFIDENTIAL” on the top of that page. The corresponding non-confidential version of those comments must be clearly marked “PUBLIC.” The file name of the non-confidential version should begin with the character “P.” Any submissions with file names that do not begin with either a “BC” or a “P” will be assumed to be public and will be made publicly available through <https://www.regulations.gov>. Commenters submitting business confidential information are encouraged to scan a hard copy of the non-confidential version to create an image of the file, rather than submitting a digital copy with redactions applied, to avoid inadvertent redaction errors which could enable the public to read business confidential information.

See the respective rules for detailed instructions on how to submit comments.

- *SME IFR:* www.regulations.gov, docket number BIS–2023–0016–0001 (ref. 0694–AJ23)
- *AC/S IFR:* www.regulations.gov, docket number BIS–2022–0025–0052 (ref. 0694–A194)

FOR FURTHER INFORMATION CONTACT:

- For general questions, contact Regulatory Policy Division, Office of Exporter Services, Bureau of Industry and Security, U.S. Department of Commerce at 202–482–2440 or by email: RPD2@bis.doc.gov.

- For Category 3 technical questions, contact Carlos Monroy at 202–482–3246 or RPD2@bis.doc.gov.

- For Category 4 or 5 technical questions, contact Aaron Amundson at 202–482–0707 or RPD2@bis.doc.gov.

SUPPLEMENTARY INFORMATION:

Background

On October 17, 2023, BIS released interim final rules (IFR) “Export Controls on Semiconductor Manufacturing Items” (SME IFR) (88 FR 73424, October 25, 2023) and “Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections” (AC/S IFR) (88 FR 73458, October 25, 2023). This rule corrects inadvertent errors contained in these rules as described below and makes additional clarifications.

I. Corrections for “Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections” (AC/S IFR) (88 FR 73458, October 25, 2023)

A. Non-CCL Corrections

A.1. Revisions to § 740.2

In § 740.2 paragraph (a)(9)(ii) introductory text, there is an incorrect citation to § 740.10(a)(3)(v), which should read § 740.10(a)(2)(iv), which prohibits exports and reexports of replacement parts to a destination specified in Country Group E:1. BIS is removing the referenced citation, because whether the specific paragraph is cited here or not, the regulatory text’s reference to § 740.10 is sufficient to indicate a restriction on the use of License Exception RPL. In addition, not citing to the specific paragraph will avoid the need for future corrections if the paragraph is moved again in License Exception RPL. The paragraph is also amended to reference License Exception Advanced Computing Authorized (ACA). Lastly, this paragraph is amended to add a reference to entities headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5, wherever located, thereby clarifying that exports, reexports, or transfers (in-country) of the items specified in § 740.2(a)(9)(ii)(A) or (B) may only be made through the license exceptions specified therein, including License Exception NAC/ACA.

A.2. Revisions to § 740.8 Notified Advanced Computing (NAC) and Advanced Computing Authorized (ACA)

This rule revises the header of § 740.8 to reference License Exception ACA in addition to License Exception NAC. BIS has separated License Exception NAC into two separate license exceptions that will reside in the same section of the EAR § 740.8: Notified Advanced Computing (NAC) will authorize exports and reexports of specified items to Macau and destinations in Country Group D:5 and entities headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5, wherever located, that require a notification to BIS, while Advanced Computing Authorized (ACA) will authorize exports, reexports, and transfers (in-country) of specified items to destinations in Country Group D:1 or D:4 (except Macau and destinations specified in Country Group D:5) that do

not require a notification to BIS. License Exception ACA will also authorize transfers (in-country) to Macau and destinations in Country Group D:5, and entities headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5, that do not require a notification to BIS. Please note that all license exceptions are also subject to the restrictions in § 740.2 and part 746 of the EAR, which would remove eligibility for embargoed and sanctioned countries, *e.g.*, Belarus, Cuba, Russia, Iran, and Syria.

In paragraph (a) introductory text, this rule updates the scope of License Exceptions NAC and ACA with regard to types of shipments, country scope, and scope of coverage for the respective license exceptions.

Paragraph (a)(1) is amended to clarify that all exports, reexports, or transfers (in-country) made pursuant to License Exceptions NAC or ACA require a written purchase order unless specifically exempted. The last sentence of paragraph (a)(1) is amended to indicate that while exports or reexports of commercial samples are not subject to the purchase order requirement, such transactions *may* be obligated to comply with paragraph (a)(2) and removes the phrase “are obligated to comply.” This change is necessary because for example, commercial sample shipments to a D:1 country under License Exception ACA would not require a notification, but such a shipment to Macau or a destination specified in Country Group D:5 under License Exception NAC would require notification.

Unlike the written purchase order requirement in paragraph (a)(1), which is required for all exports, reexports, and transfers (in-country) made under License Exceptions NAC or ACA unless specifically exempted, the notification requirement in paragraph (a)(2) only applies in specific circumstances related to License Exception NAC.

Paragraph (a)(2) is newly divided into two sections. In paragraph (a)(2)(i), this rule clarifies that the NAC notification requirement applies not only to exports or reexports to Macau or a destination specified in Country Group D:5, but also to entities headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5, wherever located. The NAC notification requirement does not apply to: exports or reexports to destinations in Country Group D:1 or D:4 (except Macau or destinations specified in Country Group D:5 or to an entity headquartered in or with an ultimate parent headquartered in those

destinations) or transfers (in-country) within any destination, which are under the scope of License Exception ACA.

In paragraph (a)(2)(ii), this rule clarifies the circumstances when one NAC notification will cover multiple exports or reexports. You may submit one NAC notification that will cover multiple exports or reexports when: the export or reexport made under License Exception NAC is to the same end user and for the same item(s) and as long as the total dollar value and quantity of the shipments do not exceed the amounts stated on the notification. This rule also clarifies that for notifications that cover multiple shipments: the dollar value and quantity on the notification do not need to match the dollar value and quantity on the purchase order submitted to BIS; the notification’s quantity and dollar value amounts may be estimates of future sales; and prior to export or reexport you must have a purchase order for every shipment made against the NAC notification.

This rule also adds a new paragraph (a)(3) to clarify that for ECCNs 5A002.z, 5A004.z, or 5D002.z, all License Exception Encryption commodities, software, and technology (ENC) requirements under § 740.17 of the EAR must also be met for eligibility under License Exceptions NAC or ACA. This assures that certain processes and procedures outlined under License Exception ENC are not circumvented with the use of License Exceptions NAC or ACA.

Paragraph (b) is amended to add references to License Exception ACA. Paragraph (b)(1) is also renumbered as paragraph (b) consistent with the changes to paragraph (b)(2) described below.

Paragraph (b)(2) restriction to use NAC or ACA by or for military end uses/users is removed because it is redundant to paragraph (b)(1) (now paragraph (b)), because that paragraph already states that, except for only § 744.23(a)(3), NAC or ACA cannot be used if there is a license requirement under part 744 or 746.

In paragraph (c) “NAC Prior notification procedures,” this rule makes a clarification to paragraph (c)(1) to specify that the NAC notification submitted in SNAP-R must include certain technical specs for performance capacity, such as Total Processing Performance (TPP), performance density, as well as a data sheet or other documentation showing the intended design goal and how it is marketed, to allow for BIS to determine if the item in question otherwise meets the criteria for an item eligible for License Exception NAC.

In paragraph (c)(2) “Action by BIS,” this rule corrects and clarifies the NAC notification process. The AC/S IFR stated that BIS would notify you if you may use NAC. However, this rule clarifies that after the notification has been registered in SNAP-R and within twenty-five calendar days, BIS will inform you if a license is required. If BIS has not contacted you, then System for Tracking Export License Applications (STELA) (<https://snapr.bis.doc.gov/stela>) will, on the twenty-fifth calendar day following the date of registration, provide either confirmation that you can use License Exception NAC and a NAC confirmation number to be submitted in AES or confirmation that you cannot use License Exception NAC and you must apply for a license to continue with the transaction.

Also in paragraph (c)(2) “Action by BIS,” this correction rule removes the last sentence that stated, “License Exception NAC eligibility does not exempt you from other licensing requirements under the EAR, such as those based on “knowledge” of a prohibited end use or end user as referenced in general prohibition five (part 736 of the EAR) and set forth in part 744 of the EAR,” because it does not speak to a BIS action.

In paragraph (c)(3) “Status of pending NAC notification requests,” this rule moves the third sentence about steps BIS will take to inform you about the use of NAC, to paragraph (c)(2), because it concerns an action by BIS. In addition, this rule clarifies the last sentence by adding “of NAC status” so that the sentence now reads, “BIS may alternatively provide such confirmation of NAC status by email, telephone, fax, courier service, or other means.”

This rule adds a new paragraph (c)(4) to inform the public of three events that would delay the processing of a NAC notification and temporarily stop the twenty-five day processing clock. If there is a lapse in appropriations funding, then BIS would stop the processing of these notifications until funding has been restored. If BIS experiences a catastrophic event, such as an extreme weather event that impacts government services, then the processing of notifications would be delayed. If for some reason BIS experiences some multi-day processing system failure, then it would not be able to continue processing the NAC notification. In such an event, BIS would post a notification to the public on the BIS website.

A.3. Revisions to § 744.23

This rule amends paragraph (c) of § 744.23 to state that License Exceptions

in § 740.2(a)(9)(i) and (ii) of the EAR may overcome the license requirements imposed by § 744.23(a)(4) and (a)(3)(i) of the EAR, respectively. BIS is making this change to harmonize with other provisions in the EAR authorizing the use of certain license exceptions. Changes to § 744.23(a)(4) are discussed in section II.B of this rule.

BIS is also amending paragraph (d) to segregate the various license review policies into new paragraphs for easier readability. Paragraph (d) retains the factors that BIS will take into account as well as the applicability of contract sanctity. New paragraph (d)(1) indicates a presumption of denial for Macau and destinations in Country Group D:5 and any entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5, unless either paragraph (d)(2) or (3) applies. New paragraph (d)(2) indicates a presumption of approval for end users headquartered in the United States or a destination specified in Country Group A:5 or A:6, that are not majority-owned by an entity headquartered in either Macau or a destination specified in Country Group D:5. New paragraph (d)(3)(i) provides a case-by-case policy for items specified in ECCN 3A090, 4A090, 3A001.z, 4A003.z, 4A004.z, 4A005.z, 5A002.z, 5A004.z, 5A992.z, 5D002.z, or 5D992.z, except for items designed or marketed for use in a datacenter and meeting the parameters of 3A090.a. These items are less sensitive integrated circuits and computers that do not warrant a presumption of denial license review policy. New paragraph (d)(3)(ii) now indicates a case-by-case review policy for SME subject to the license requirements of § 744.23, when there is SME not subject to the license requirements of § 744.23 that performs the same function as the SME that is subject to the license requirements of § 744.23. Case-by-case policy is appropriate for such items because denying the license may not further national security when there is an option for SME that is not subject to the license requirement and performs the same function. Lastly, there is a case-by-case policy in paragraph (d)(3)(iii) for items not specified in paragraph (d)(1) or (2) or (d)(3)(i) or (ii).

A.4. Revisions to § 744.6 Restrictions on Specific Activities of “U.S. Persons”

BIS is adding EUV masks (ECCN 3B001.j) and associated software and technology to the control in paragraph (c)(2)(iii) for SME, because it was unintentionally excluded from controls. EUV masks are required for lithography

and lithography is a critical technology for advance-node IC production.

This rule reformats the license review policy in paragraph (e)(3) by cascading the paragraphs for easier readability. BIS is also adding a new exception from the presumption of denial license review policy that is added by this rule in paragraph (e)(3)(ii)(A), which is a case-by-case policy for items specified in ECCN 3A090, 4A090, 3A001.z, 4A003.z, 4A004.z, 4A005.z, 5A002.z, 5A004.z, 5A992.z, 5D002.z, or 5D992.z, except for items designed or marketed for use in a datacenter and meeting the parameters of 3A090.a. These items are less sensitive integrated circuits and computers, *i.e.*, not “advanced-node integrated circuits” or computers containing “advanced-node integrated circuits”, that do not warrant a presumption of denial license review policy. There is also another new exception from the presumption of denial policy in paragraph (e)(3)(ii)(B) that sets forth a case-by-case review policy for activities involving an item subject to the license requirements of paragraph (c)(2) where there is an item that performs the same function as an item meeting the license requirements of paragraph (c)(2). Lastly, paragraph (e)(3)(ii)(C) clarifies that there is a case-by-case policy for all other applications not specified in paragraphs (e)(3)(i) or (e)(ii)(A) or (B).

B. Correction to Model Certification in Supplement No. 1 to Part 734

In supplement no. 1 to part 734—Model Certification for Purposes of the FDP Rule, this rule revises the model criteria included under paragraph (b)(2)(viii) for consistency with the country scope specified in § 734.9(i)(2), which specifies the country scope applies to the People’s Republic of China (PRC) and Macau. This rule removes the reference to Macau or a destination specified in Country Group D:5 in paragraph (b)(2)(viii) of supplement no. 1 to part 734 and replaces that with the correct country scope of the PRC and Macau for consistency with § 734.9(i)(2).

C. Correction to § 742.15(a)

Because there was an error in amendatory instruction 21 in the AC/S IFR, this rule revises § 742.15(a)(1), licensing requirements for Encryption items, by adding back the third sentence, which had been inadvertently removed in the AC/S IFR, and removing the last sentence of that paragraph, which repeats the sentence before.

D. Removing References to Note 4 to 3A090

In ECCN 3A090, this rule makes a correction to Note 3 to 3A090 to remove a reference to Note 4 to 3A090 because that note does not exist. During the drafting process of the AC/S IFR, ECCN 3A090 included a Note 4 that was subsequently removed prior to the AC/S IFR being published. The cross reference to Note 4 in Note 3 in the Related Controls paragraph in 4A090 was not updated at the time Note 4 to 3A090 was removed. For the same reason, this rule revises the Related Controls paragraph in the following ten ECCNs to remove references to Note 4 to 3A090. Specifically, this rule corrects the Related Controls paragraphs under 3A001, 4A003, 4A004, 4A005, 4A090, 5A002, 5A992, 5A004, 5D002 and 5D992 to remove the cross reference to Note 4 to 3A090. These cross references to the non-existent Note 4 to 3A090 do not cause a substantive issue, but may cause confusion for exporters, reexporters, or transferors, so this rule corrects that in each of these ECCNs.

E. Restoring Controls for ECCNs That Contain .z Paragraphs

This rule restores controls in the license requirement table of ECCNs 3A001, 3D001, 3E001, 4A003, 4A004, 4A005, 4D001, 4E001, 5A002, 5A004, 5D002, and 5E002, by removing the exceptions for .z paragraphs from the national security (NS), missile technology, nuclear proliferation, and/or crime control license requirement paragraphs. Prior to the AC/S IFR, these items were controlled for NS, missile technology, nuclear proliferation, and/or crime control reasons, however, when the .z paragraphs were added, items that contained either 3A090 or 4A090 items were only controlled for RS reasons, which changed the country scope of the license requirements for these items. For example, in ECCN 4A003, there is a license requirement for NS reasons for exports, reexports, or transfers (in-country) to destinations specified in NS column 1 (NS:1), which is a worldwide control, except for Canada. However, if the commodity specified in ECCN 4A003, such as a computer, contained an integrated circuit specified in ECCN 3A090, then it only required a license for RS reasons to destinations in Country Groups D:1, D:4, and D:5 that are not also in Country Groups A:5 or A:6, which would in essence implement a decontrol for these computers to many destinations, including those specified in Country Group A:5 and A:6. Therefore, this rule restores the other reasons for control for

items that meet the specifications in .z paragraphs of these ECCNs.

F. Maintaining the Status Quo for License Exception Eligibility for Certain Destinations

The addition of .z paragraphs to certain ECCNs was intended to make it easier for exporters, reexporters, and transferors of items subject to certain end-use controls to more easily distinguish those items from other items controlled under the same ECCNs. It was not intended to affect the control status or license exception availability of those other items. As a conforming change to the restoration of controls for .z paragraphs (explained in the section above), and in order to retain the status quo for EAR license exception eligibility when not restricted by § 740.2(a)(9)(ii), this rule adds a new note to the License Exception section of each of the ECCNs that have or impose controls on .z items: 3A001, 3D001, 3E001, 4A003, 4A004, 4A005, 4D001, 4E001, 5A002, 5A992, 5A004, 5D002, 5D992, 5E002, and 5E992. The new note refers the public to see § 740.2(a)(9)(ii) of the EAR for license exception restrictions for .z ECCNs, because only the license exceptions in § 740.2(a)(9)(ii) may be used for exports, reexports, or transfers (in-country) of .z ECCNs to destinations specified in Country Groups D:1, D:4, or D:5 (excluding any destination also specified in Country Groups A:5 or A:6) or to an entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5, wherever located. When destined elsewhere, all other applicable license exceptions may be used unless otherwise restricted.

BIS is making these changes to ensure the .z paragraphs will not be used to circumvent regime controls under the respective .z ECCNs (for instance, by inserting a chip to make the item a .z item and thereby eligible for License Exceptions NAC or ACA, provided the export, reexport, or transfer (in-country) also otherwise meet the applicable terms and conditions of License Exceptions NAC or ACA). However, BIS also does not want the addition of a .z paragraph under one of the respective .z ECCNs to otherwise narrow the scope of license exception eligibility that applied to these items prior to the addition of the .z paragraphs to these respective ECCNs, unless the destination is specified in Country Group D:1, D:4 or D:5 (excluding destinations in Country Group A:5 or A:6), or to an entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5, wherever located.

License Exception STA eligibility is preserved for .z ECCNs by removing restrictions under STA restriction paragraphs for .z ECCNs. However, like all license exception use for .z ECCNs, STA may not overcome the license exception restrictions in § 740.2(a)(9)(ii) of the EAR.

G. Revisions to 3A001

This rule adds four new .z paragraphs to ECCN 3A001 to make a distinction of those paragraphs controlled for NS:1, RS:1, MT:1, and NP:1 reasons. Paragraph 3A001.z.1 is added to control “Monolithic Microwave Integrated Circuit” (“MMIC”) amplifiers described in 3A001.b.2 and discrete microwave transistors in 3A001.b.3, except those 3A001.b.2 and b.3 items being exported or reexported for use in civil telecommunications applications and that also meet or exceed the performance parameters in ECCN 3A090, which are controlled under the NS:1, RS:1, RS (§ 742.6(a)(6)(iii) of the EAR), MT:1, and AT:1 license requirements paragraphs. Paragraph 3A001.z.2 is added to control commodities that are described in 3A001.a.1.a when usable in “missiles” that also meet or exceed the performance parameters in ECCN 3A090; and to 3A001.a.5.a when “designed or modified” for military use, hermetically sealed and rated for operation in the temperature range from below -54°C to above $+125^{\circ}\text{C}$ and that also meet or exceed the performance parameters in ECCN 3A090. Corresponding changes are made to the NS:2, RS (§ 742.6(a)(6)(iii) of the EAR), MT:1, and AT:1 license requirements paragraphs. Paragraph 3A001.z.3 is added to control pulse discharge capacitors described in 3A001.e.2 and superconducting solenoidal electromagnets in 3A001.e.3 that meet or exceed the technical parameters in 3A201.a and 3A201.b, respectively and that also meet or exceed the performance parameters in 3A090, which are controlled under the NS:2, RS (§ 742.6(a)(6)(iii) of the EAR), NP:1, and AT:1 license requirements. Paragraph 3A001.z.4 is added to control all other commodities specified in ECCN 3A001 that meet or exceed the parameters of ECCN 3A090.

This rule also fixes typos to ECCN 3A001 paragraphs .b.11.b and .c.1.b.2.

H. Revisions to ECCN 3D001

The NS license requirement paragraph in the License Requirements section of ECCN 3D001 is corrected by restoring NS:1 license requirements to software for commodities controlled by

3A001.z by adding 3A001.z to the NS:1 licensing paragraph.

I. Revision to ECCN 3E001 License Requirements and Reasons for Control

In 3E001, this rule adds RS to the reason for control paragraph and the exception clauses for 3A001.z are removed from the NS:1, MT:1, and NP:1 license requirement paragraphs to restore those controls for commodities controlled in ECCN 3A001 that also meet or exceed the parameters in ECCN 3A090.

J. Addition of Missing Paragraph 4A090.b

In ECCN 4A090, BIS inadvertently reserved paragraph 4A090.b. This correction rule adds 4A090.b to control computers, “electronic assemblies,” and “components” containing integrated circuits, any of which meets or exceeds the limits in 3A090.b. The rule also amends the technical note in this ECCN to clarify the use of the term computers. The NAC/ACA eligibility paragraph for ECCN 4A090 already includes text that makes such commodities eligible for NAC/ACA.

K. Revisions to ECCN 4E001

In 4E001.a, this rule removes an incorrect phrase “or “software” controlled under 4D001 (for 4A090)” because software for 4A090 is controlled in ECCN 4D090, not 4D001.

L. Revisions to ECCN 5D002 and 5D992

This rule corrects the Related Control paragraphs of ECCN 5D002 and 5D992 by replacing the references to non-existent paragraphs 3D001.z and 4D001.z with correct references to “ECCNs 3D001 as it applies to “software” for commodities controlled by 3A001.z and 3A090 and 4D001 as it applies to “software” for commodities controlled by 4A003.z, 4A004.z, and 4A005.z.”

M. Revisions to ECCN 5E992 and 5E002

This rule corrects the Reason for Control paragraph in the License Requirement section of ECCN 5E992 and 5E002 by adding “RS” to indicate the regional stability license requirements in the License Requirements table.

N. Revision to Supplement No. 6 to Part 774—Sensitive List

In paragraphs 3(iv) and (v), this rule removes the phrase “and equipment described under 3A002.g.2 that are controlled under 3A002.z” because BIS decided against adding a 3A002.z paragraph, so none was created.

II. “Export Controls on Semiconductor Manufacturing Items” (SME IFR) (88 FR 73424, October 25, 2023)

A. Corrections to ECCN 3B001 and 3B991

In ECCN 3B001, this rule corrects the scientific unit in paragraphs d.4.d.2 by replacing 13.33 kPa with 13.33 Pa; and in paragraph d.5 replacing 450 Mpa with 450 MPa. In paragraph f.1.b.2.b, this rule replaces 2.4 nm with 2.40 nm for consistency with how the other numbers are listed in paragraph f.1.b.2. In paragraph o.2, this rule adds a missing “or” after cobalt (Co) and before tungsten.

In ECCN 3B001, this rule corrects the scope of items subject to § 742.4(a)(4) national security controls and § 742.6(a)(6)(i) regional stability controls by adding ECCN 3B001.j “Mask “substrate blanks” with multilayer reflector structure consisting of molybdenum and silicon . . .” and being ““Specially designed” for “Extreme Ultraviolet” (“EUV”) lithography” and compliant with SEMI Standard P37. BIS inadvertently left this paragraph outside the scope of §§ 740.2(a)(9)(i), 742.4(a)(4), 742.6(a)(6)(i), 744.6(c)(2)(iii), and 744.23(a)(4) of the EAR and ECCN 3D002 heading and license requirements table.

The heading of 3B991 is corrected to remove the reference to ECCN 3B090, which was removed from the CCL by the SME IFR.

B. Revision of § 744.23(a)(4)

BIS is revising the scope of the exceptions for masks in § 744.23(a)(4)(i), because it unintentionally excepted EUV masks in 3B001.j, as well as equipment in 3B991.b.2. Therefore, the exceptions are narrowed to include 3B001.h, and 3B991.b.2.a through .b.

BIS received several comments asking for clarification on the application of § 744.23(a)(4) to the incorporation of CCL-listed items into foreign-made items that are themselves destined for the “development” or “production” of specified SME in Macau or a destination specified in Country Group D:5, because other paragraphs in § 744.23 included incorporation provisions, but this one did not. The definition of “production” in § 772.1 of the EAR includes the term integration, which BIS believes already captures the physical incorporation of one item into another or the joining of two items. That being said, BIS is revising § 744.23(a)(4) by adding a new paragraph (a)(4)(ii) to distinguish between direct exports, reexports, and transfers (in-country) in (a)(4)(i) and indirect exports, reexports, transfers (in-

country) in (a)(4)(ii) for the “development” or “production,” by an entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5. This revision is being done to address concerns about continued support for indigenous “development” and “production” of front-end integrated circuit “production” equipment in Macau and destinations in Country Group D:5 countries—and by companies headquartered in those countries. Consistent with BIS’s revised topic responses addressing “incorporation,” paragraph (a)(4)(ii) requires a license for the export, reexport, or transfer (in-country) of any item subject to the EAR and specified on the CCL to any destination when there is “knowledge” that (A) the item is for “development” or “production” of a foreign-made item, whether subject to the EAR or not, that is specified in an ECCN listed in paragraph (a)(4)(i); (B) when the foreign-made item is for “development” or “production” of any initial or subsequent foreign-made item, whether subject to the EAR or not, specified in an ECCN listed in paragraph (a)(4)(i); and (C) the “development” or “production” is by an entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5. BIS is taking this step to address certain scenarios where the initial exporter, reexporter, or transferor has “knowledge” that its items subject to the EAR and specified on the CCL will ultimately support the indigenous “development” or “production” of SME in Macau and destinations specified in Country Group D:5. At the same time, BIS has limited the scope of this control to circumstances involving the “development” or “production” of front-end SME items by entities that are headquartered in, or whose ultimate parent company is headquartered in, Macau or a destination specified in Country Group D:5. BIS also adds a new Note 2 to explain that, to the extent new paragraph (a)(4)(ii) controls the “development” or “production” of front-end SME produced at the direction of entities headquartered outside of Macau or Country Group D:5 destinations, the Temporary General License (TGL) in General Order 4, Supplement No. 1 to Part 736, is available, provided the other requirements of that section are satisfied. Further, for clarity, BIS notes that this clarification does not control the use of items subject to the EAR for the “development” or “production” of

foreign-made items outside of Macau or Country Group D:5 destinations that are ultimately destined for the “development” or “production” of CCL Category 3A items, and not the 3B or related 3D and 3E items specified in (a)(4)(i). Rather, this scenario is addressed under § 744.23(a)(2), which is the subject of extensive discussion in the revised topic responses, described below in Section C.

Even though new paragraph (a)(4)(ii) excludes the need to evaluate whether the foreign-made item that the exported, reexported, or transferred item is being integrated into is subject to the EAR, it does not eliminate the need to assess separately whether any foreign-made item is subject to the EAR under other provisions, including the De Minimis Rule or Foreign Direct Product Rule, which may impose other independent license requirements.

C. Clarification to BIS Responses to Certain Public Comment Topics

BIS received a number of comments asking for clarification to responses to four topics in the SME IFR. For ease of reference, BIS provides copies of the original topics below, numbered as they were in the SME IFR.

Topic 45: A commenter asked BIS to clarify whether a license would be required under § 744.23(a)(4) (former § 744.23(a)(2)(v)) to export an item subject to the EAR to a third party Original Equipment Manufacturer (OEM) in a third country, where there is “knowledge” at the time of the export that the item would be incorporated into a foreign-made 3B991 item (not subject to the EAR) by the OEM in the third country, and that the OEM would then send the 3B991 item to a manufacturer of Category 3 items in China. This commenter noted that § 744.23(a) does not expressly state that the “End Use Scope” includes the end use of the item into which the exported item is incorporated, and this differs from other EAR provisions, such as the foreign direct product (FDP) rules under §§ 734.9 and 744.23(a)(1)(ii)(B), which expressly include “incorporated into” as part of the end-use scope.

BIS response: Paragraph (a) of § 744.23 requires a license for items subject to the EAR when “you have “knowledge” at the time of export, reexport, or transfer (in-country) that the item is destined for a destination, end use, or type of end user described in paragraphs (a)(1) through (4) of this section.” While paragraphs (a)(2) through (4) apply to Category 3 items (among others), paragraph (a)(2) is specific to the “development” and “production” of “advanced-node

integrated circuits,” paragraph (a)(3) is specific to advanced computing items, and paragraph (a)(4) applies to the “development” and “production” of certain Category 3 “production” equipment. As the license requirements for § 744.23(a)(2) through (4) each cover different circumstances, the license requirements for § 744.23(a)(2) through (3) are distinct from the license requirements of § 744.23(a)(4).

The EAR defines “production” as including all production stages such as integration. As noted in response to Topic 19 in the SME IFR, “[a]uthorization would be required if there is “knowledge” at the time of export, reexport, or transfer (in-country) that an item on the CCL will ultimately be used (including by incorporation into another item such as a “part” or “component”) in the “development” or “production” of specified Group 3B ECCN equipment in Macau or a destination specified in Country Group D:5.” Thus, paragraph (a)(4) of § 744.23 does require a license to export, reexport, or transfer (in-country) an item specified on the Commerce Control List (CCL) for the “production” of certain equipment, components, assemblies, and accessories specified in Category 3, even when the export, reexport, or transfer (in-country) is to a third party OEM in a country other than Macau or a destination specified in Country Group D:5 when there is “knowledge” that the export, reexport or transfer (in-country) is for the “production” of semiconductor production equipment specified in the ECCNs enumerated in § 744.23(a)(4)(i), and is by an entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5.

Paragraphs (a)(2) and (3) only apply when there is “knowledge” that the item is destined to the production of certain integrated circuits—“advanced-node integrated circuits” and advanced computing items (including integrated circuits described in ECCNs 3A001.z and 3A090)—not the equipment to produce integrated circuits described in paragraph (a)(4). The party incorporating the item must still determine whether the foreign-made item is subject to the EAR under the *de minimis* or foreign-direct product (FDP) rules. See §§ 734.4 and 734.9 of the EAR; see also supplement no. 2 to part 734—Guidelines for *De Minimis* Rules (“Part 744 of the EAR should not be used to identify controlled U.S. content for purposes of determining the applicability of the *de minimis* rules.”). Refer to BIS’s responses to Topics 46, 47, and 49 in this Section and Topic 19

of the SME IFR for additional guidance on the topic of incorporation or integration under § 744.23(a)(2) and (4). In addition, exporters may not self-blind or disregard “knowledge” that the transaction is structured to avoid a license requirement. For example, an exporter may not ignore readily available information that the customer will integrate the exported item into an item destined for Macau or a Country Group D:5 destination for the production of equipment and items specified in § 744.23(a)(4)(i).

Topic 46: A commenter asked BIS to confirm how far back up the supply chain the licensing obligation extends for an export of an item to a third party for use in developing or producing a whole new foreign-made item that will only later be used in the development or production of ICs at a covered facility (*i.e.*, a facility where “advanced-node integrated circuits” are produced). This commenter described a scenario in which someone exports an item to produce a foreign-made item, which will be used to produce another foreign-made item, which will later be used at a covered fabrication facility, and asked whether the original export is caught by the new licensing obligations if there is knowledge that this supply chain will ultimately result in the creation of an item used to produce ICs at a covered fabrication facility. The commenter further inquired about the transfer outside the United States of items subject to the EAR to produce foreign-made items when only a small percentage of the foreign-made items will be for use at a covered fabrication facility. Specifically, the commenter asked whether BIS takes the position that 100% of all such transfers require a license by the foreign parties even when only an unknown small percentage will be used in the production of items that will ultimately be destined to covered fabrication facilities.

BIS response: BIS notes that § 744.23(a)(2) does not prohibit transactions involving the incorporation, as it pertains to *de minimis* rules, or integration of items subject to the EAR into foreign-made items, assuming such incorporation does not separately trigger a license requirement (*e.g.*, under § 734.9 (Foreign Direct Product (FDP) Rules) or § 744.23). In any case, the reexporter or transferor must separately assess whether a license would be required to reexport or transfer (in-country) the foreign-made item under § 734.4 (*De Minimis* Rule), including for items ineligible for *de minimis* under § 734.4(a), or other provisions of the EAR. However, if an

OEM restructures its supply chain to avoid a license requirement, then a license would still be required under § 744.23(a)(2), without which such restructuring indicates an attempt to evade or otherwise violate the EAR.

With respect to the commenter’s second question about in-country transfers of items that are not intended for incorporation into foreign-made items, but rather direct use in a prohibited end use, a license would be required for the portion or percentage of items for which there is “knowledge” that the items are destined for use in a prohibited end use. This is true at any point in the supply chain at which such “knowledge” exists. In the case of Category 3B, 3C, 3D, and 3E items subject to the EAR, a license could also be required under § 744.23(a)(2)(ii), even if the production technology node of the “facility” at which they will be used is unknown.

Topic 47: A commenter noted that clarification of § 744.23(a)(2)(iv), which has been redesignated as paragraph (a)(2)(ii) in the SME and AC/S IFRs, is needed if this imposes an affirmative duty to know or otherwise be subject to a license requirement. The commenter asks whether this means that a license is required when a company is exporting products to China and cannot confirm whether the semiconductor fabrication facility is producing products that meet the specified criteria in paragraphs (a)(2)(iii)(A) through (C), which has been redesignated as a part 772 defined term “advanced-node ICs” in the SME and AC/S IFRs.

BIS response: Yes, if the exporter, reexporter, or transferor has “knowledge” that an item identified in § 744.23(a)(2)(iv) (*i.e.*, Category 3B, 3C, 3D and 3E items), which was redesignated as paragraph (a)(2)(ii) in the SME IFR, will be used in the “development” or “production” of integrated circuits (ICs) in Macau or a destination specified in Country Group D:5, but does not have “knowledge” of whether such ICs are or will be “advanced-node integrated circuits,” a license is required.

This BIS response would also apply to a similar scenario in which an exporter, reexporter, or transferor has positive “knowledge” that their 3B/C/D/E products are used by some number of entities engaged in legacy development/production, but they do not know how 100% of their product is used (*e.g.*, because they are an upstream distributor and cannot keep track of all of it). A license is required to ship 100% of the items, unless the exporter, reexporter, or transferor can determine which items of the 100% will not be used in the

“development” or “production” of ICs in Macau or a destination specified in Country Group D:5, which would be excluded from the license requirement under § 744.23(a)(2)(iv), redesignated as paragraph (a)(2)(ii) in the SME IFR. Note that this response assumes the upstream transactions involve items that will be used directly in a prohibited end use, and not incorporated into foreign-made items. A license would not necessarily be required to ship an item destined for incorporation into a foreign-made item, assuming, *e.g.*, that the exporter has not self-blinded or possesses “knowledge” that the transaction is structured to avoid a license requirement. As described in response to Topics 45, 46, and 49, absent such “knowledge,” subsequent incorporation is addressed by other provisions of the EAR. See § 734.4 (*De Minimis* Rule) and § 734.9 (Foreign Direct Product (FDP) Rules); see also § 770.2(a)(2) (“An anti-friction bearing or bearing system physically incorporated in a segment of a machine or in a complete machine prior to shipment loses its identity as a bearing.”) and § 770.2(b)(1) (describing components that do not require a license “provided that the [items] are normal and usual components of the machine or equipment or that the physical incorporation is not used as a device to evade the requirement for a license.”); BIS, Advisory Opinion dated September 14, 2009 (addressing the “second incorporation principle”), available at <https://www.bis.doc.gov/index.php/documents/advisory-opinions/531-second-incorporation-rule/file>.

Topic 49: A commenter requested BIS clarify whether it would be sufficient under § 744.6 to have an end user certify that the exported item will not be used in “the “development” or “production” in China of any “parts,” “components,” or “equipment” specified under ECCN 3B001, 3B002, 3B090, 3B611, 3B991, or 3B992.

BIS response: BIS interprets this comment to refer to the end-use control under § 744.23(a)(4) (former § 744.23(a)(2)(v)), as there is no U.S. person control under § 744.6(c)(2) with the characteristics described by the commenter. Sufficient due diligence will vary depending on the specific facts of a transaction. Exporters, reexporters, and transferors may not self-blind or structure transactions to avoid a license requirement. However, BIS distinguishes between self-blinding or structuring to avoid a license requirement and the established legitimate incorporation of items subject to the EAR into foreign-made items, consistent with the requirements and

prohibitions of the *De Minimis* Rule and FDP Rules. See BIS’s responses to Topics 45, 46, and 47 for additional guidance on this question.

D. Clarification of § 744.23(d) To Improve Understanding

This rule revises § 744.23(d) (License review standards) for clarity to address a question BIS has received on the two exceptions that are specified for the presumption of denial license review policy included in the SME IFR by making the following changes. This rule removes the last sentence of paragraph (d), which specified general provisions that apply to all license reviews under paragraph (d) and redesignates that as the first sentence of paragraph (d) introductory text. Because this text applies to all of paragraph (d) it will be clearer to include this as the introductory text to paragraph (d). The license review policy is split into three new paragraphs: (d)(1) presumption of denial policy; (d)(2) presumption of approval policy; and (d)(3) case-by-case policy, which consists of three paragraphs.

Paragraph (d)(1) (Presumption of denial) is revised by adding “entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5,” which aligns with the destination-based presumption of denial policy for Macau and destinations in Country Group D:5.

This rule also adds new paragraph (d)(2) as the first exception, which specifies that license applications for end users headquartered in the United States or a destination in Country Group A:5 or A:6, that are not majority-owned by an entity headquartered in either Macau or a destination specified in Country Group D:5 are reviewed under a presumption of approval. The SME IFR included this exception, but redesignating this exception into its own paragraph will make it easier to understand.

This rule also adds a new paragraph (d)(3) (Case-by-case), to move the case-by-case license review policy that was included in the SME IFR into its own paragraph for ease of reference. In addition, BIS is adding in new paragraph (d)(3)(i) a case-by-case policy for certain enumerated items, excluding items designed or marketed for use in a datacenter and meeting the parameters of ECCN 3A090.a. This rule adds under new paragraph (d)(3)(ii), a case-by-case policy for license applications for when there is a foreign-made item available that is not subject to the license requirements in § 744.23 and performs the same function as the item subject to

the EAR. Lastly, for clarity and as a conforming change, this rule adds the phrase “not specified in paragraphs (d)(1), (2), or (3)(i) or (ii)” at the end of new paragraph (d)(3)(iii) to clarify that the case-by-case license review policy applies to all other license applications that are not already addressed in paragraph (d)(1) or (2) or (d)(3)(i) or (ii).

Savings Clause

Shipments of items removed from license exception eligibility or eligibility for export, reexport or transfer (in-country) without a license as a result of this regulatory action that were on dock for loading, on lighter, laden aboard an exporting carrier, or en route aboard a carrier to a port of export, on April 4, 2024, pursuant to actual orders for exports, reexports and transfers (in-country) to a foreign destination, may proceed to that destination under the previous license exception eligibility or without a license so long as they have been exported, reexported or transferred (in-country) before May 6, 2024. Any such items not actually exported, reexported or transferred (in-country) before midnight, on May 6, 2024, require a license in accordance with this interim final rule.

Export Control Reform Act of 2018

On August 13, 2018, the President signed into law the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which included the Export Control Reform Act of 2018 (ECRA) (codified, as amended, at 50 U.S.C. 4801–4852). ECRA provides the legal basis for BIS’s principal authorities and serves as the authority under which BIS issues this rule.

Rulemaking Requirements

1. Executive Orders 12866, 13563, and 14094 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects and distributive impacts and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits and of reducing costs, harmonizing rules, and promoting flexibility. This interim final rule has been designated a “significant regulatory action” under Executive Order 12866.

2. Notwithstanding any other provision of law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork

Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA), unless that collection of information displays a currently valid Office of Management and Budget (OMB) Control Number.

This rule involves the following OMB-approved collections of information subject to the PRA:

- 0694–0088, “Multi-Purpose Application,” which carries a burden hour estimate of 29.4 minutes for a manual or electronic submission;
- 0694–0096 “Five Year Records Retention Period,” which carries a burden hour estimate of less than 1 minute;
- 0694–0122, “Licensing Responsibilities and Enforcement;” and
- 0607–0152 “Automated Export System (AES) Program,” which carries a burden hour estimate of 3 minutes per electronic submission.

The AC/S IFR will affect the collection under control number 0694–0088, for the multipurpose application because of the addition of the notification requirement for exports and reexports to China in order to use new License Exception Notified Advanced Computing (NAC) under § 740.8 of the EAR. BIS estimates that License Exception NAC notification will result in an increase of 3,000 multi-purpose applications submitted annually to BIS and an increase of 950 burden hours under this collection. BIS also anticipates the submission annually of 200 license applications as a result of the revision to license requirements included in the AC/S IFR, but because the original estimate that was included in the October 7 IFR (*i.e.*, that BIS estimates that these new controls under the EAR imposed by the October 7 IFR would result in an increase of 1,700 license applications submitted annually to BIS) was higher than the actual number of license applications BIS has received over the first year of the October IFR changes being in place, BIS did not anticipate any changes in these estimates as a result of the changes included in the AC/S IFR for license applications submitted to BIS as a result of the AC/S IFR with the one exception of the increase in burden hours for the License Exception NAC notifications, which was not accounted for in the October 7 IFR because License Exception NAC was not part of the EAR at that time.

The AC/S IFR will affect the information collection under control number 0607–0152, for filing EEI in AES because this rule adds § 758.1(g)(5) to impose a requirement for identifying .z items by “items” level classification in the EEI filing in AES. This change is not anticipated to result in a change in

the burden under this collection because filers are already required to provide a description in the Commodity description block in the EEI filing in AES. This regulation also involves a collection previously approved by the OMB under control number 0694–0122, “Licensing Responsibilities and Enforcement” because this rule under the revision to § 758.6(a)(2) will require the ECCN(s) for any 3A001.z, 3A090, 4A003.z, 4A004.z, 4A005.z, 4A090, 5A002.z, 5A004.z, 5A992.z to be included on the commercial invoice, similar to the previous requirement to include the “600 series” and 9x515 ECCNs on the commercial invoice. BIS does not anticipate a change in the total burden hours associated with the PRA and OMB control number 0694–0122 as a result of this rule.

Additional information regarding these collections of information—including all background materials—can be found at <https://www.reginfo.gov/public/do/PRAMain> by using the search function to enter either the title of the collection or the OMB Control Number.

3. This rule does not contain policies with federalism implications as that term is defined in Executive Order 13132.

4. Pursuant to section 1762 of ECRA (50 U.S.C. 4821), this action is exempt from the Administrative Procedure Act (APA) (5 U.S.C. 553) requirements for notice of proposed rulemaking, opportunity for public participation, and delay in effective date. While section 1762 of ECRA provides sufficient authority for such an exemption, this action is also independently exempt from these APA requirements because it involves a military or foreign affairs function of the United States (5 U.S.C. 553(a)(1)). However, BIS is not only accepting comments on both the SME and AC/S IFRs, but has in this rule extended the comment period by 30 days for both rules.

5. Because a notice of proposed rulemaking and an opportunity for public comment are not required to be given for this rule by 5 U.S.C. 553, or by any other law, the analytical requirements of the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq.*, are not applicable. Accordingly, no regulatory flexibility analysis is required, and none has been prepared.

List of Subjects

15 CFR Parts 732 and 748

Administrative practice and procedure, Exports, Reporting and recordkeeping requirements.

15 CFR Part 734

Administrative practice and procedure, Exports, Inventions and patents, Research, Science and technology.

15 CFR Parts 740 and 758

Administrative practice and procedure, Exports, Reporting and recordkeeping requirements.

15 CFR Part 742

Exports, Terrorism.

15 CFR Part 744

Exports, Reporting and recordkeeping requirements, Terrorism.

15 CFR Parts 746 and 774

Exports, Reporting and recordkeeping requirements.

15 CFR Parts 736, 770, and 772

Exports.

For the reasons stated in the preamble, parts 732, 734, 736, 740, 742, 744, 746, 748, 758, 770, 772, and 774 of the Export Administration Regulations (15 CFR parts 730 through 774) are amended as follows:

PART 734—SCOPE OF THE EXPORT ADMINISTRATION REGULATIONS

- 1. The authority citation for part 734 continues to read as follows:

Authority: 50 U.S.C. 4801–4852; 50 U.S.C. 4601 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 13020, 61 FR 54079, 3 CFR, 1996 Comp., p. 219; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; E.O. 13637, 78 FR 16129, 3 CFR, 2014 Comp., p. 223; Notice of November 1, 2023, 88 FR 75475.

- 2. Supplement no. 1 to part 734 is amended by revising paragraph (b)(2)(viii) to read as follows:

Supplement No. 1 to Part 734—Model Certification for Purposes of the FDP Rule

* * * * *

(b) * * *

(2) * * *

(viii) Country and end-use scope of § 734.9(i)(2), *i.e.*, used in the design, “development,” “production,” operation, installation (including on-site installation), maintenance (checking), repair, overhaul, or refurbishing of, a “supercomputer” located in or destined to the People’s Republic of China (PRC) or Macau; or incorporated into, or used in the “development,” or “production,” of any “part,” “component,” or “equipment” that will be used in a

“supercomputer” located in or destined to the PRC or Macau;

* * * * *

PART 740—LICENSE EXCEPTIONS

■ 3. The authority citation for part 740 continues to read as follows:

Authority: 50 U.S.C. 4801–4852; 50 U.S.C. 4601 *et seq.*; 50 U.S.C. 1701 *et seq.*; 22 U.S.C. 7201 *et seq.*; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783.

■ 4. Section 740.2 is amended by revising paragraphs (a)(9)(i) and (a)(9)(ii) introductory text to read as follows:

§ 740.2 Restrictions on all License Exceptions.

* * * * *

(a) * * *

(9) (i) The item is controlled under ECCN 3B001.a.4, c, d, f.1.b, j to p, 3B002.b or c, or associated software and technology in ECCN 3D001, 3D002, 3D003, or 3E001 and is being exported, reexported, or transferred (in-country) to or within either Macau or a destination specified in Country Group D:5 of supplement no. 1 to this part, and the license exception is other than License Exception GOV, restricted to eligibility under the provisions of § 740.11(b).

(ii) The item is identified in paragraph (a)(9)(ii)(A) or (B) of this section, is being exported, reexported, or transferred (in-country) to or within a destination specified in Country Group D:1, D:4, or D:5, excluding any destination also specified in Country Groups A:5 or A:6, or to an entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5, wherever located, and the license exception is other than: TMP, restricted to eligibility under the provisions of § 740.9(a)(6); NAC/ACA, under the provisions of § 740.8; RPL, under the provisions of § 740.10; GOV, restricted to eligibility under the provisions of § 740.11(b); or TSU under the provisions of § 740.13(a) and (c). Items restricted to eligibility only for the foregoing license exceptions are:

* * * * *

■ 5. Section 740.8 is revised to read as follows:

§ 740.8 Notified Advanced Computing (NAC) and Advanced Computing Authorized (ACA).

(a) *Eligibility requirements.* License Exception NAC authorizes the export and reexport of any item classified in ECCN 3A090, 4A090, 3A001.z, 4A003.z, 4A004.z, 4A005.z, 5A002.z, 5A004.z, 5A992.z, 5D002.z, or 5D992.z, except for items designed or marketed for use in a

datacenter and meeting the parameters of 3A090.a, to Macau and Country Group D:5 or an entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5, wherever located. License Exception ACA authorizes the export, reexport, and transfer (in-country) of any item classified in ECCN 3A090, 4A090, 3A001.z, 4A003.z, 4A004.z, 4A005.z, 5A002.z, 5A004.z, 5A992.z, 5D002.z, or 5D992.z, except for items designed or marketed for use in a datacenter and meeting the parameters of 3A090.a, to or within any destination specified in Country Groups D:1 and D:4 (except Macau, a destination in Country Group D:5, or an entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5, wherever located), as well as transfers (in-country) within Macau and destinations in Country Group D:5. These license exceptions may be used provided the export, reexport, or transfer (in-country) meets all of the applicable criteria identified under this paragraph (a) and none of the restrictions in paragraph (b) of this section.

(1) *Written purchase order.* Prior to any exports, reexports, and transfers (in-country) made pursuant to License Exceptions NAC or ACA you must obtain a written purchase order unless specifically exempted in this paragraph. Commercial samples are not subject to this purchase order requirement, but such transactions may be obligated to comply with paragraph (a)(2) of this section.

(2) *NAC Notification to BIS—(i) Notification requirement.* Prior to any exports or reexports to Macau or a destination specified in Country Group D:5 or to an entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5, wherever located, the exporter or reexporter must notify BIS in accordance with the procedures set forth in paragraph (c) of this section.

(ii) *Multiple exports and reexports.* For multiple exports or reexports under License Exception NAC to the same end user and for the same item(s), the exporter or reexporter need only notify BIS prior to the first export or reexport, as long as the total dollar value and quantity of the shipments do not exceed the amounts stated on the notification. The dollar value and quantity on the notification do not need to match the dollar value and quantity on the purchase order; the notification's quantity and dollar value amounts may be based on estimates of future sales.

However, prior to export or reexport you must have a purchase order for every shipment made against the NAC notification. BIS will provide further information on the notification process in the policy guidance tab on the BIS website.

(3) *In relation to License Exception ENC and ECCNs 5A002.z, 5A004.z, or 5D002.z.* For exports, reexports, or transfer (in-country) of ECCNs 5A002.z, 5A004.z, or 5D002.z, all License Exception Encryption commodities, software, and technology (ENC) requirements under § 740.17 of this part must also be met for eligibility under License Exceptions NAC or ACA.

(b) *Restrictions.* No exports, reexports, or transfers (in-country) may be made under License Exception NAC or ACA that are subject to a license requirement under part 744 or 746 of the EAR, except for a license required under § 744.23(a)(3) for reexports or exports to any destination other than those specified in Country Groups D:1, D:4, or D:5 (excluding any destination also specified in Country Groups A:5 or A:6) for an entity that is headquartered in, or whose ultimate parent company is headquartered in, either Macau or a destination specified in Country Group D:5.

(c) *NAC Prior notification procedures—(1) Procedures.* At least twenty-five calendar days prior to exports or reexports using License Exception NAC, you must provide prior notification under License Exception NAC by submitting a completed application in SNAP–R in accordance with § 748.1 of the EAR. The following blocks must be completed, as appropriate: Blocks 1, 2, 3, 4, 5 (by marking box 5 export license or reexport license), 9, 14, 16, 17, 18, 19, 21, 22(a), (d), (e), (f), (g), (h), (i), (j), 23, 24, and 25 according to the instructions described in supplement no. 1 to part 748 of the EAR. Box 9 under special purpose must include NAC. The application must include certain information to allow for BIS to determine if the item in question otherwise meets the criteria for an item eligible for License Exception NAC. Required information to include in the NAC submission is as follows:

(i) Total Processing Performance of the item, as defined in ECCN 3A090;

(ii) Performance density of the item, as defined in ECCN 3A090; and

(iii) Data sheet or other documentation showing how the item is designed and marketed (in particular, whether it is designed or marketed for datacenter use).

(2) *Action by BIS for NAC notifications.* After the notification has

been registered in SNAP–R and within twenty-five calendar days after registration, BIS will inform you if a license is required. If BIS has not contacted you, then System for Tracking Export License Applications (STELA) (<https://snapr.bis.doc.gov/stela>) will, on the twenty-fifth calendar day following the date of registration, provide either confirmation that you can use License Exception NAC and a NAC confirmation number to be submitted in AES or confirmation that you cannot use License Exception NAC and you must apply for a license to continue with the transaction.

(3) *Status of pending NAC notification requests.* Log into BIS’s STELA for information about the status of your pending NAC notification or to verify the status in BIS’s Simplified Network Applications Processing Redesign (SNAP–R) System. STELA will provide the date the NAC notification is registered. BIS may alternatively provide such confirmation of NAC status by email, telephone, fax, courier service, or other means.

(4) *Actions that delay processing of NAC notifications.* Below are circumstances that will delay the processing of your NAC notification, *i.e.*, temporarily stop the twenty-five day processing clock for NAC notification:

- (i) Lapse in appropriations.
- (ii) Catastrophic event (*e.g.*, an extreme weather event that impacts government services).
- (iii) Multi-day processing system failure.

* * * * *

PART 742—CONTROL POLICY—CCL BASED CONTROLS

■ 6. The authority citation for part 742 is revised to read as follows:

Authority: 50 U.S.C. 4801–4852; 50 U.S.C. 4601 *et seq.*; 50 U.S.C. 1701 *et seq.*; 22 U.S.C. 3201 *et seq.*; 42 U.S.C. 2139a; 22 U.S.C. 7201 *et seq.*; 22 U.S.C. 7210; Sec. 1503, Pub. L. 108–11, 117 Stat. 559; E.O. 12058, 43 FR 20947, 3 CFR, 1978 Comp., p. 179; E.O. 12851, 58 FR 33181, 3 CFR, 1993 Comp., p. 608; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Presidential Determination 2003–23, 68 FR 26459, 3 CFR, 2004 Comp., p. 320; Notice of November 1, 2023, 88 FR 75475 (November 3, 2023).

■ 7. Section 742.4 is amended by revising paragraph (a)(4) to read as follows:

§ 742.4 National security.

- (a) * * *

(4) *Certain semiconductor manufacturing equipment and associated software and technology.* A license is required for exports, reexports, and transfers (in-country) to or within either Macau or a destination specified in Country Group D:5 in supplement no. 1 to part 740 of the EAR of items specified in 3B001.a.4, c, d, f.1.b, j to p; 3B002.b and c; 3D001 (for 3B001.a.4, c, d, f.1.b, j to p, 3B002.b and c); 3D002 (for 3B001 a.4, c, d, f.1.b, j to p, 3B002.b and c); or 3E001 (for 3B001.a.4, c, d, f.1.b, j to p, 3B002.b and c). The license requirements in this paragraph (a)(4) do not apply to deemed exports or deemed reexports.

* * * * *

■ 8. Section 742.6 is amended by revising paragraph (a)(6)(i) to read as follows:

§ 742.6 Regional stability.

- (a) * * *
- (6) * * *

(i) *Exports, reexports, transfers (in-country) to or within Macau or Country Group D:5.* A license is required for items specified in ECCNs 3B001.a.4, c, d, f.1.b, j to p, 3B002.b and c; and associated software and technology in 3D001 (for 3B001.a.4, c, d, f.1.b, j to p, 3B002.b and c), 3D002 (for 3B001.a.4, c, d, f.1.b, j to p, 3B002.b and c), and 3E001 (for 3B001.a.4, c, d, f.1.b, j to p, 3B002.b and c) being exported, reexported, or transferred (in-country) to or within Macau or a destination specified in Country Group D:5 in supplement no. 1 to part 740 of the EAR.

* * * * *

■ 9. Section 742.15 is amended by revising paragraph (a)(1) to read as follows:

§ 742.15 Encryption items.

- (a) * * *

(1) *Licensing requirements.* A license is required to export or reexport encryption items (“EI”) classified under ECCN 5A002, 5A004, 5D002.a, .c.1 or .d (for equipment and “software” in ECCNs 5A002 or 5A004, 5D002.c.1); or 5E002 for “technology” for the “development,” “production,” or “use” of commodities or “software” controlled for EI reasons in ECCNs 5A002, 5A004 or 5D002, and “technology” classified under 5E002.b to all destinations, except Canada. Refer to part 740 of the EAR, for license exceptions that apply to certain encryption items, and to § 772.1 of the EAR for definitions of encryption items and terms. Most encryption items may be exported under the provisions of License Exception

ENC set forth in § 740.17 of the EAR. Following classification or self-classification, items that meet the criteria of Note 3 to Category 5—Part 2 of the Commerce Control List (the “mass market” note), are classified under ECCN 5A992 or 5D992 and are no longer subject to this Section (see § 740.17 of the EAR). Before submitting a license application, please review License Exception ENC to determine whether this license exception is available for your item or transaction. For exports, reexports, or transfers (in-country) of encryption items that are not eligible for a license exception, you must submit an application to obtain authorization under a license or an Encryption Licensing Arrangement.

* * * * *

PART 744—CONTROL POLICY: END-USER AND END-USE BASED

■ 10. The authority citation for part 744 is revised to read as follows:

Authority: 50 U.S.C. 4801–4852; 50 U.S.C. 4601 *et seq.*; 50 U.S.C. 1701 *et seq.*; 22 U.S.C. 3201 *et seq.*; 42 U.S.C. 2139a; 22 U.S.C. 7201 *et seq.*; 22 U.S.C. 7210; E.O. 12058, 43 FR 20947, 3 CFR, 1978 Comp., p. 179; E.O. 12851, 58 FR 33181, 3 CFR, 1993 Comp., p. 608; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13099, 63 FR 45167, 3 CFR, 1998 Comp., p. 208; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; E.O. 13224, 66 FR 49079, 3 CFR, 2001 Comp., p. 786; ; Notice of September 7, 2023, 88 FR 62439 (September 11, 2023), Notice of November 1, 2023, 88 FR 75475.

■ 11. Section 744.6 is amended by revising paragraphs (c)(2)(iii) and (e)(3) to read as follows:

§ 744.6 Restrictions on specific activities of “U.S. persons.”

* * * * *

- (c) * * *
- (2) * * *

(iii) *Semiconductor manufacturing equipment.* To or within either Macau or a destination specified in Country Group D:5, any item not subject to the EAR and meeting the parameters of ECCNs 3B001.a.4, c, d, f.1.b, j to p; 3B002.b and c; 3D001 (for 3B001.a.4, c, d, f.1.b, j to p, 3B002.b and c); 3D002 (for 3B001 a.4, c, d, f.1.b, j to p, 3B002.b and c); or 3E001 (for 3B001.a.4, c, d, f.1.b, j to p, 3B002.b and c) regardless of end use or end user.

* * * * *

- (e) * * *

(3) Applications for licenses submitted pursuant to the notice of a license requirement set forth in paragraph (c)(2) of this section will be reviewed in accordance with the policies described in paragraphs (e)(1)

through (3) of this section. License review will take into account factors including technology level, customers, compliance plans, and contract sanctity.

(i) *Presumption of denial.*

Applications will be reviewed with a presumption of denial for Macau and destinations specified in Country Group D:5 and entities headquartered or whose ultimate parent is headquartered in Macau or destinations specified in Country Group D:5, unless paragraph (e)(3)(ii) of this section applies.

(ii) *Case-by-case.* Applications will be reviewed with a case-by-case policy for license applications that meet either of the following conditions:

(A) For items specified in ECCN 3A090, 4A090, 3A001.z, 4A003.z, 4A004.z, 4A005.z, 5A002.z, 5A004.z, 5A992.z, 5D002.z, or 5D992.z, except for items designed or marketed for use in a datacenter and meeting the parameters of 3A090.a;

(B) For activities involving an item subject to the license requirements of paragraph (c)(2) of this section where there is an item not subject to the license requirements of paragraph (c)(2) that performs the same function as an item meeting the license requirements of paragraph (c)(2); or

(C) For all other applications not specified in paragraph (e)(3)(i) or (e)(3)(ii)(A) or (B) of this section.

■ 12. Section 744.23 is amended by revising paragraphs (a)(4), (c), and (d) to read as follows:

§ 744.23 “Supercomputer,” “advanced-node integrated circuits,” and semiconductor manufacturing equipment end use controls.

* * * * *

(a) * * *

(4) *Semiconductor manufacturing equipment (SME) and “components,” “assemblies,” and “accessories.”* A license is required for export, reexport, or transfer (in-country) if either paragraph (a)(4)(i) or (ii) of this section applies.

(i) *Directly destined to Macau and Country Group D:5.* Any item subject to the EAR and specified on the CCL when destined to or within either Macau or a destination specified in Country Group D:5 for the “development” or “production” of “front-end integrated circuit “production” equipment” and “components,” “assemblies,” and “accessories” therefor specified in ECCN 3B001 (except 3B001.g and .h), 3B002, 3B611, 3B991 (except 3B991.b.2.a through .b), 3B992, or associated “software” and “technology” in 3D or 3E of the CCL.

(ii) *Indirect exports, reexports, or transfers (in-country).* Any item subject

to the EAR and specified on the CCL for export, reexport, or transfer (in-country), if all of the following apply:

(A) The item is for “development” or “production” of a foreign-made item, whether subject to the EAR or not, that is specified in an ECCN listed in paragraph (i);

(B) When the foreign-made item is for “development” or “production” of any initial or subsequent foreign-made item, whether subject to the EAR or not, specified in an ECCN listed in paragraph (a)(4)(i) of this section; and

(C) The “development” or “production” is by an entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5.

Note 1 to paragraph (a)(4): Front-end integrated circuit “production” equipment includes equipment used in the production stages from a blank wafer or substrate to a completed wafer or substrate (*i.e.*, the integrated circuits are processed but they are still on the wafer or substrate). If there is a question at the time of export, reexport, or transfer (in-country) about whether equipment is used in front-end integrated circuit “production,” you may submit an advisory opinion request to BIS pursuant to § 748.3(c) of the EAR for clarification.

Note 2 to paragraph (a)(4): For transactions involving “development” or “production” in Macau or a destination specified in Country Group D:5 by an entity that is headquartered in Macau or a destination specified in Country Group D:5, but the “development” or “production” is undertaken at the direction of an entity headquartered in the United States or a destination specified in Country Group A:5 or A:6, refer to General Order No. 4 in Supp. No. 1 to Part 736 (Temporary General License—Less restricted SME “parts,” “components,” or “equipment”).

* * * * *

(c) *License exceptions.* No license exceptions may overcome the prohibition described in paragraph (a) of this section, except the prohibitions in paragraphs (a)(4) and (a)(3)(i) of this section may be overcome by license exceptions in § 740.2(a)(9)(i) or (ii) of the EAR, respectively.

(d) *License review standards.* License review will consider several factors including technology level, customers, compliance plans, and contract sanctity.

(1) *Presumption of denial.*

Applications will be reviewed with a presumption of denial for Macau and destinations specified in Country Group

D:5 and any entity headquartered in, or with an ultimate parent headquartered in, Macau or a destination specified in Country Group D:5, unless either paragraph (d)(2) or (3) applies.

(2) *Presumption of approval.*

Applications will be reviewed with a presumption of approval for end users headquartered in the United States or a destination specified in Country Group A:5 or A:6, that are not majority-owned by an entity headquartered in either Macau or a destination specified in Country Group D:5.

(3) *Case-by-case.* There is a case-by-case license review policy for license applications that meet one of the following conditions:

(i) For items specified in ECCN 3A090, 4A090, 3A001.z, 4A003.z, 4A004.z, 4A005.z, 5A002.z, 5A004.z, 5A992.z, 5D002.z, or 5D992.z, except for items designed or marketed for use in a datacenter and meeting the parameters of 3A090.a;

(ii) For items subject to the license requirements of this section where there is a foreign-made item that is not subject to the license requirements of this section and performs the same function as an item subject to the EAR license requirements of this section; or

(iii) For all other applications not specified in paragraph (d)(1) or (2) or (d)(3)(i) or (ii).

PART 774—THE COMMERCE CONTROL LIST

■ 13. The authority citation for part 774 continues to read as follows:

Authority: 50 U.S.C. 4801–4852; 50 U.S.C. 4601 *et seq.*; 50 U.S.C. 1701 *et seq.*; 10 U.S.C. 8720; 10 U.S.C. 8730(e); 22 U.S.C. 287c, 22 U.S.C. 3201 *et seq.*; 22 U.S.C. 6004; 42 U.S.C. 2139a; 15 U.S.C. 1824; 50 U.S.C. 4305; 22 U.S.C. 7201 *et seq.*; 22 U.S.C. 7210; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783.

■ 14. Supplement no. 1 to part 774 is amended by revising ECCNs 3A001, 3A090, 3B001, 3B991, 3D001, 3D002, 3E001, 4A003, 4A004, 4A005, 4A090, 4D001, 4E001, 5A002, 5A992, 5A004, 5D002, 5D992, 5E002, and 5E992 to read as follows:

Supplement No. 1 to Part 774—The Commerce Control List

* * * * *

3A001 Electronic items as follows (see List of Items Controlled).

Reason for Control: NS, RS, MT, NP, AT

Control(s)	Country chart (see Supp. No. 1 to part 738)	Control(s)	Country chart (see Supp. No. 1 to part 738)	the destinations listed in Country Group A:5 or A:6 (See Supplement No.1 to part 740 of the EAR).
NS applies to “Monolithic Microwave Integrated Circuit” (“MMIC”) amplifiers in 3A001.b.2 and discrete microwave transistors in 3A001.b.3, except those 3A001.b.2 and b.3 items being exported or reexported for use in civil telecommunications applications; and 3A001.z.1.	NS Column 1.	NP applies to pulse discharge capacitors in 3A001.e.2 and superconducting solenoidal electromagnets in 3A001.e.3 that meet or exceed the technical parameters in 3A201.a and 3A201.b, respectively; and 3A001.z.3.	NP Column 1.	List of Items Controlled
NS applies to entire entry.	NS Column 2.	AT applies to entire entry.	AT Column 1.	<i>Related Controls:</i> (1) See Category XV of the USML for certain “space-qualified” electronics and Category XI of the USML for certain ASICs, ‘transmit/receive modules,’ or ‘transmit modules’ ‘subject to the ITAR’ (see 22 CFR parts 120 through 130). (2) See also 3A090, 3A101, 3A201, 3A611, 3A991, and 9A515.
RS applies “Monolithic Microwave Integrated Circuit” (“MMIC”) amplifiers in 3A001.b.2 and discrete microwave transistors in 3A001.b.3, except those 3A001.b.2 and b.3 items being exported or reexported for use in civil telecommunications applications; and 3A001.z.1.	RS Column 1.	Reporting Requirements: See § 743.1 of the EAR for reporting requirements for exports under 3A001.b.2 or b.3 under License Exceptions, and Validated End-User authorizations. License Requirements: See § 744.17 of the EAR for additional license requirements for microprocessors having a processing speed of 5 GFLOPS or more and an arithmetic logic unit with an access width of 32 bit or more, including those incorporating “information security” functionality, and associated “software” and “technology” for the “production” or “development” of such microprocessors.		<i>Related Definitions:</i> ‘Microcircuit’ means a device in which a number of passive or active elements are considered as indivisibly associated on or within a continuous structure to perform the function of a circuit. For the purposes of integrated circuits in 3A001.a.1, 5×10^3 Gy(Si) = 5×10^5 Rads (Si); 5×10^6 Gy (Si)/s = 5×10^8 Rads (Si)/s.
RS applies to 3A001.z.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.	List Based License Exceptions (See Part 740 for a Description of All License Exceptions)		<i>Items:</i>
MT applies to 3A001.a.1.a when usable in “missiles”; and to 3A001.a.5.a when “designed or modified” for military use, hermetically sealed and rated for operation in the temperature range from below -54°C to above $+125^\circ\text{C}$; and 3A001.z.2.	MT Column 1.	LVS: N/A for MT, NP; N/A for “Monolithic Microwave Integrated Circuit” (“MMIC”) amplifiers in 3A001.b.2, discrete microwave transistors in 3A001.b.3, and 3A001.z.1, except those that are being exported or reexported for use in civil telecommunications applications. Yes for: \$1500: 3A001.c \$3000: 3A001.b.1, b.2 (exported or reexported for use in civil telecommunications applications), b.3 (exported or reexported for use in civil telecommunications applications), b.9, .d, .e, .f, .g, and z.1 (exported or reexported for use in civil telecommunications applications). \$5000: 3A001.a (except a.1.a and a.5.a when controlled for MT), b.4 to b.7, and b.12. GBS: Yes for 3A001.a.1.b, a.2 to a.14 (except a.5.a when controlled for MT), b.2 (exported or reexported for use in civil telecommunications applications), b.8 (except for “vacuum electronic devices” exceeding 18 GHz), b.9., b.10, .g, .h, .i, and z.1 (exported or reexported for use in civil telecommunications applications). NAC/ACA: Yes, for 3A001.z. Note: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for ECCN 3A001.z.		Note 1: Integrated circuits include the following types: —“Monolithic integrated circuits”; —“Hybrid integrated circuits”; —“Multichip integrated circuits”; —Film type integrated circuits, including silicon-on-sapphire integrated circuits”; —“Optical integrated circuits”; —“Three dimensional integrated circuits”; —“Monolithic Microwave Integrated Circuits” (“MMICs”). a.1. Integrated circuits designed or rated as radiation hardened to withstand any of the following: a.1.a. A total dose of 5×10^3 Gy (Si), or higher; a.1.b. A dose rate upset of 5×10^6 Gy (Si)/s, or higher; or a.1.c. A fluence (integrated flux) of neutrons (1 MeV equivalent) of 5×10^{13} n/cm ² or higher on silicon, or its equivalent for other materials; Note: 3A001.a.1.c does not apply to Metal Insulator Semiconductors (MIS). a.2. “Microprocessor microcircuits,” “microcomputer microcircuits,” microcontroller microcircuits, storage integrated circuits manufactured from a compound semiconductor, analog-to-digital converters, integrated circuits that contain analog-to-digital converters and store or process the digitized data, digital-to-analog converters, electro-optical or “optical integrated circuits” designed for “signal processing”, field programmable logic devices, custom integrated circuits for which either the function is unknown or the control status of the equipment in which the integrated circuit will be used in unknown, Fast Fourier Transform (FFT) processors, Static Random-Access Memories (SRAMs), or ‘non-volatile memories,’ having any of the following: Technical Note: For the purposes of 3A001.a.2, ‘non-volatile memories’ are memories with data retention over a period of time after a power shutdown. a.2.a. Rated for operation at an ambient temperature above 398 K (+125 °C); a.2.b. Rated for operation at an ambient temperature below 218 K (–55 °C); or
		Special Conditions for STA		
		STA: License Exception STA may not be used to ship any item in 3A001.b.2 or b.3, except those that are being exported or reexported for use in civil telecommunications applications, to any of		

a.2.c. Rated for operation over the entire ambient temperature range from 218 K (−55 °C) to 398 K (+125 °C);

Note: 3A001.a.2 does not apply to integrated circuits designed for civil automobile or railway train applications.

a.3. “Microprocessor microcircuits”, “microcomputer microcircuits” and microcontroller microcircuits, manufactured from a compound semiconductor and operating at a clock frequency exceeding 40 MHz;

Note: 3A001.a.3 includes digital signal processors, digital array processors and digital coprocessors.

a.4. [Reserved]

a.5. Analog-to-Digital Converter (ADC) and Digital-to-Analog Converter (DAC) integrated circuits, as follows:

a.5.a. ADCs having any of the following:

a.5.a.1. A resolution of 8 bit or more, but less than 10 bit, with a “sample rate” greater than 1.3 Giga Samples Per Second (GSPS);

a.5.a.2. A resolution of 10 bit or more, but less than 12 bit, with a “sample rate” greater than 600 Mega Samples Per Second (MSPS);

a.5.a.3. A resolution of 12 bit or more, but less than 14 bit, with a “sample rate” greater than 400 MSPS;

a.5.a.4. A resolution of 14 bit or more, but less than 16 bit, with a “sample rate” greater than 250 MSPS; or

a.5.a.5. A resolution of 16 bit or more with a “sample rate” greater than 65 MSPS;

N.B.: For integrated circuits that contain analog-to-digital converters and store or process the digitized data see 3A001.a.14.

Technical Notes: For the purposes of 3A001.a.5.a:

1. A resolution of n bit corresponds to a quantization of 2^n levels.

2. The resolution of the ADC is the number of bits of the digital output that represents the measured analog input. Effective Number of Bits (ENOB) is not used to determine the resolution of the ADC.

3. For “multiple channel ADCs”, the “sample rate” is not aggregated and the “sample rate” is the maximum rate of any single channel.

4. For “interleaved ADCs” or for “multiple channel ADCs” that are specified to have an interleaved mode of operation, the “sample rates” are aggregated and the “sample rate” is the maximum combined total rate of all of the interleaved channels.

a.5.b. Digital-to-Analog Converters (DAC) having any of the following:

a.5.b.1. A resolution of 10-bit or more but less than 12-bit, with an ‘adjusted update rate’ of exceeding 3,500 MSPS; or

a.5.b.2. A resolution of 12-bit or more and having any of the following:

a.5.b.2.a. An ‘adjusted update rate’ exceeding 1,250 MSPS but not exceeding 3,500 MSPS, and having any of the following:

a.5.b.2.a.1. A settling time less than 9 ns to arrive at or within 0.024% of full scale from a full scale step; or

a.5.b.2.a.2. A ‘Spurious Free Dynamic Range’ (SFDR) greater than 68 dBc (carrier) when synthesizing a full scale analog signal of 100 MHz or the highest full scale analog signal frequency specified below 100 MHz; or

a.5.b.2.b. An ‘adjusted update rate’ exceeding 3,500 MSPS;

Technical Notes: For the purposes of 3A001.a.5.b:

1. ‘Spurious Free Dynamic Range’ (SFDR) is defined as the ratio of the RMS value of the carrier frequency (maximum signal component) at the input of the DAC to the RMS value of the next largest noise or harmonic distortion component at its output.

2. SFDR is determined directly from the specification table or from the characterization plots of SFDR versus frequency.

3. A signal is defined to be full scale when its amplitude is greater than -3 dBfs (full scale).

4. ‘Adjusted update rate’ for DACs is:

a. For conventional (non-interpolating) DACs, the ‘adjusted update rate’ is the rate at which the digital signal is converted to an analog signal and the output analog values are changed by the DAC. For DACs where the interpolation mode may be bypassed (interpolation factor of one), the DAC should be considered as a conventional (non-interpolating) DAC.

b. For interpolating DACs (oversampling DACs), the ‘adjusted update rate’ is defined as the DAC update rate divided by the smallest interpolating factor. For interpolating DACs, the ‘adjusted update rate’ may be referred to by different terms including:

- input data rate
- input word rate
- input sample rate
- maximum total input bus rate
- maximum DAC clock rate for DAC clock input.

a.6. Electro-optical and “optical integrated circuits”, designed for “signal processing” and having all of the following:

a.6.a. One or more than one internal “laser” diode;

a.6.b. One or more than one internal light detecting element; and

a.6.c. Optical waveguides;

a.7. ‘Field programmable logic devices’ having any of the following:

a.7.a. A maximum number of single-ended digital input/outputs of greater than 700; or

a.7.b. An ‘aggregate one-way peak serial transceiver data rate’ of 500 Gb/s or greater;

Note: 3A001.a.7 includes:

—Complex Programmable Logic Devices (CPLDs);

—Field Programmable Gate Arrays (FPGAs);

—Field Programmable Logic Arrays (FPLAs);

—Field Programmable Interconnects (FPICs).

N.B.: For integrated circuits having field programmable logic devices that are combined with an analog-to-digital converter, see 3A001.a.14.

Technical Notes: For the purposes of 3A001.a.7:

1. Maximum number of digital input/outputs in 3A001.a.7.a is also referred to as maximum user input/outputs or maximum available input/outputs, whether the integrated circuit is packaged or bare die.

2. ‘Aggregate one-way peak serial transceiver data rate’ is the product of the peak serial one-way transceiver data rate times the number of transceivers on the FPGA.

a.8. [Reserved]

a.9. Neural network integrated circuits;

a.10. Custom integrated circuits for which the function is unknown, or the control status of the equipment in which the integrated circuits will be used is unknown to the manufacturer, having any of the following:

a.10.a. More than 1,500 terminals;

a.10.b. A typical “basic gate propagation delay time” of less than 0.02 ns; or

a.10.c. An operating frequency exceeding 3 GHz;

a.11. Digital integrated circuits, other than those described in 3A001.a.3 to 3A001.a.10 and 3A001.a.12, based upon any compound semiconductor and having any of the following:

a.11.a. An equivalent gate count of more than 3,000 (2 input gates); or

a.11.b. A toggle frequency exceeding 1.2 GHz;

a.12. Fast Fourier Transform (FFT) processors having a rated execution time for an N -point complex FFT of less than $(N \log_2 N)/20,480$ ms, where N is the number of points;

Technical Note: For the purposes of 3A001.a.12, when N is equal to 1,024 points, the formula in 3A001.a.12 gives an execution time of 500 μ s.

a.13. Direct Digital Synthesizer (DDS) integrated circuits having any of the following:

a.13.a. A Digital-to-Analog Converter (DAC) clock frequency of 3.5 GHz or more and a DAC resolution of 10 bit or more, but less than 12 bit; or

a.13.b. A DAC clock frequency of 1.25 GHz or more and a DAC resolution of 12 bit or more;

Technical Note: For the purposes of 3A001.a.13, the DAC clock frequency may be specified as the master clock frequency or the input clock frequency.

a.14. Integrated circuits that perform or are programmable to perform all of the following:

a.14.a. Analog-to-digital conversions meeting any of the following:

a.14.a.1. A resolution of 8 bit or more, but less than 10 bit, with a “sample rate” greater than 1.3 Giga Samples Per Second (GSPS);

a.14.a.2. A resolution of 10 bit or more, but less than 12 bit, with a “sample rate” greater than 1.0 GSPS;

a.14.a.3. A resolution of 12 bit or more, but less than 14 bit, with a “sample rate” greater than 1.0 GSPS;

a.14.a.4. A resolution of 14 bit or more, but less than 16 bit, with a “sample rate” greater than 400 Mega Samples Per Second (MSPS); or

a.14.a.5. A resolution of 16 bit or more with a “sample rate” greater than 180 MSPS; and

a.14.b. Any of the following:

a.14.b.1. Storage of digitized data; or

a.14.b.2. Processing of digitized data;

N.B. 1: For analog-to-digital converter integrated circuits see 3A001.a.5.a.

N.B. 2: For field programmable logic devices see 3A001.a.7.

Technical Notes: For the purposes of 3A001.a.14:

1. A resolution of n bit corresponds to a quantization of 2^n levels.

2. The resolution of the ADC is the number of bits of the digital output of the ADC that

represents the measured analog input. Effective Number of Bits (ENOB) is not used to determine the resolution of the ADC.

3. For integrated circuits with non-interleaving “multiple channel ADCs”, the “sample rate” is not aggregated and the “sample rate” is the maximum rate of any single channel.

4. For integrated circuits with “interleaved ADCs” or with “multiple channel ADCs” that are specified to have an interleaved mode of operation, the “sample rates” are aggregated and the “sample rate” is the maximum combined total rate of all of the interleaved channels.

b. Microwave or millimeter wave items, as follows:

Technical Note: For the purposes of 3A001.b, the parameter peak saturated power output may also be referred to on product data sheets as output power, saturated power output, maximum power output, peak power output, or peak envelope power output.

b.1. “Vacuum electronic devices” and cathodes, as follows:

Note 1: 3A001.b.1 does not control “vacuum electronic devices” designed or rated for operation in any frequency band and having all of the following:

a. Does not exceed 31.8 GHz; and

b. Is “allocated by the ITU” for radio-communications services, but not for radio-determination.

Note 2: 3A001.b.1 does not control non-“space-qualified” “vacuum electronic devices” having all the following:

a. An average output power equal to or less than 50 W; and

b. Designed or rated for operation in any frequency band and having all of the following:

1. Exceeds 31.8 GHz but does not exceed 43.5 GHz; and

2. Is “allocated by the ITU” for radio-communications services, but not for radio-determination.

b.1.a. Traveling-wave “vacuum electronic devices,” pulsed or continuous wave, as follows:

b.1.a.1. Devices operating at frequencies exceeding 31.8 GHz;

b.1.a.2. Devices having a cathode heater with a turn on time to rated RF power of less than 3 seconds;

b.1.a.3. Coupled cavity devices, or derivatives thereof, with a “fractional bandwidth” of more than 7% or a peak power exceeding 2.5 kW;

b.1.a.4. Devices based on helix, folded waveguide, or serpentine waveguide circuits, or derivatives thereof, having any of the following:

b.1.a.4.a. An “instantaneous bandwidth” of more than one octave, and average power (expressed in kW) times frequency (expressed in GHz) of more than 0.5;

b.1.a.4.b. An “instantaneous bandwidth” of one octave or less, and average power (expressed in kW) times frequency (expressed in GHz) of more than 1;

b.1.a.4.c. Being “space-qualified”; or

b.1.a.4.d. Having a gridded electron gun;

b.1.a.5. Devices with a “fractional bandwidth” greater than or equal to 10%, with any of the following:

b.1.a.5.a. An annular electron beam;

b.1.a.5.b. A non-axisymmetric electron beam; or

b.1.a.5.c. Multiple electron beams;

b.1.b. Crossed-field amplifier “vacuum electronic devices” with a gain of more than 17 dB;

b.1.c. Thermionic cathodes, designed for “vacuum electronic devices,” producing an emission current density at rated operating conditions exceeding 5 A/cm² or a pulsed (non-continuous) current density at rated operating conditions exceeding 10 A/cm²;

b.1.d. “Vacuum electronic devices” with the capability to operate in a ‘dual mode.’
Technical Note: For the purposes of 3A001.b.1.d, ‘dual mode’ means the “vacuum electronic device” beam current can be intentionally changed between continuous-wave and pulsed mode operation by use of a grid and produces a peak pulse output power greater than the continuous-wave output power.

b.2. “Monolithic Microwave Integrated Circuit” (“MMIC”) amplifiers that are any of the following:

N.B.: For “MMIC” amplifiers that have an integrated phase shifter see 3A001.b.12.

b.2.a. Rated for operation at frequencies exceeding 2.7 GHz up to and including 6.8 GHz with a “fractional bandwidth” greater than 15%, and having any of the following:

b.2.a.1. A peak saturated power output greater than 75 W (48.75 dBm) at any frequency exceeding 2.7 GHz up to and including 2.9 GHz;

b.2.a.2. A peak saturated power output greater than 55 W (47.4 dBm) at any frequency exceeding 2.9 GHz up to and including 3.2 GHz;

b.2.a.3. A peak saturated power output greater than 40 W (46 dBm) at any frequency exceeding 3.2 GHz up to and including 3.7 GHz; or

b.2.a.4. A peak saturated power output greater than 20 W (43 dBm) at any frequency exceeding 3.7 GHz up to and including 6.8 GHz;

b.2.b. Rated for operation at frequencies exceeding 6.8 GHz up to and including 16 GHz with a “fractional bandwidth” greater than 10%, and having any of the following:

b.2.b.1. A peak saturated power output greater than 10 W (40 dBm) at any frequency exceeding 6.8 GHz up to and including 8.5 GHz; or

b.2.b.2. A peak saturated power output greater than 5 W (37 dBm) at any frequency exceeding 8.5 GHz up to and including 16 GHz;

b.2.c. Rated for operation with a peak saturated power output greater than 3 W (34.77 dBm) at any frequency exceeding 16 GHz up to and including 31.8 GHz, and with a “fractional bandwidth” of greater than 10%;

b.2.d. Rated for operation with a peak saturated power output greater than 0.1 nW (–70 dBm) at any frequency exceeding 31.8 GHz up to and including 37 GHz;

b.2.e. Rated for operation with a peak saturated power output greater than 1 W (30 dBm) at any frequency exceeding 37 GHz up to and including 43.5 GHz, and with a “fractional bandwidth” of greater than 10%;

b.2.f. Rated for operation with a peak saturated power output greater than 31.62

mW (15 dBm) at any frequency exceeding 43.5 GHz up to and including 75 GHz, and with a “fractional bandwidth” of greater than 10%;

b.2.g. Rated for operation with a peak saturated power output greater than 10 mW (10 dBm) at any frequency exceeding 75 GHz up to and including 90 GHz, and with a “fractional bandwidth” of greater than 5%; or

b.2.h. Rated for operation with a peak saturated power output greater than 0.1 nW (–70 dBm) at any frequency exceeding 90 GHz;

Note 1: [Reserved]

Note 2: The control status of the “MMIC” whose rated operating frequency includes frequencies listed in more than one frequency range, as defined by 3A001.b.2.a through 3A001.b.2.h, is determined by the lowest peak saturated power output control threshold.

Note 3: Notes 1 and 2 following the Category 3 heading for product group A. Systems, Equipment, and Components mean that 3A001.b.2 does not control “MMICs” if they are “specially designed” for other applications, e.g., telecommunications, radar, automobiles.

b.3. Discrete microwave transistors that are any of the following:

b.3.a. Rated for operation at frequencies exceeding 2.7 GHz up to and including 6.8 GHz and having any of the following:

b.3.a.1. A peak saturated power output greater than 400 W (56 dBm) at any frequency exceeding 2.7 GHz up to and including 2.9 GHz;

b.3.a.2. A peak saturated power output greater than 205 W (53.12 dBm) at any frequency exceeding 2.9 GHz up to and including 3.2 GHz;

b.3.a.3. A peak saturated power output greater than 115 W (50.61 dBm) at any frequency exceeding 3.2 GHz up to and including 3.7 GHz; or

b.3.a.4. A peak saturated power output greater than 60 W (47.78 dBm) at any frequency exceeding 3.7 GHz up to and including 6.8 GHz;

b.3.b. Rated for operation at frequencies exceeding 6.8 GHz up to and including 31.8 GHz and having any of the following:

b.3.b.1. A peak saturated power output greater than 50 W (47 dBm) at any frequency exceeding 6.8 GHz up to and including 8.5 GHz;

b.3.b.2. A peak saturated power output greater than 15 W (41.76 dBm) at any frequency exceeding 8.5 GHz up to and including 12 GHz;

b.3.b.3. A peak saturated power output greater than 40 W (46 dBm) at any frequency exceeding 12 GHz up to and including 16 GHz; or

b.3.b.4. A peak saturated power output greater than 7 W (38.45 dBm) at any frequency exceeding 16 GHz up to and including 31.8 GHz;

b.3.c. Rated for operation with a peak saturated power output greater than 0.5 W (27 dBm) at any frequency exceeding 31.8 GHz up to and including 37 GHz;

b.3.d. Rated for operation with a peak saturated power output greater than 1 W (30 dBm) at any frequency exceeding 37 GHz up to and including 43.5 GHz;

b.3.e. Rated for operation with a peak saturated power output greater than 0.1 nW (-70 dBm) at any frequency exceeding 43.5 GHz; or

b.3.f. Other than those specified by 3A001.b.3.a to 3A001.b.3.e and rated for operation with a peak saturated power output greater than 5 W (37.0 dBm) at all frequencies exceeding 8.5 GHz up to and including 31.8 GHz;

Note 1: *The control status of a transistor in 3A001.b.3.a through 3A001.b.3.e, whose rated operating frequency includes frequencies listed in more than one frequency range, as defined by 3A001.b.3.a through 3A001.b.3.e, is determined by the lowest peak saturated power output control threshold.*

Note 2: *3A001.b.3 includes bare dice, dice mounted on carriers, or dice mounted in packages. Some discrete transistors may also be referred to as power amplifiers, but the status of these discrete transistors is determined by 3A001.b.3.*

b.4. Microwave solid state amplifiers and microwave assemblies/modules containing microwave solid state amplifiers, that are any of the following:

b.4.a. Rated for operation at frequencies exceeding 2.7 GHz up to and including 6.8 GHz with a “fractional bandwidth” greater than 15%, and having any of the following:

b.4.a.1. A peak saturated power output greater than 500 W (57 dBm) at any frequency exceeding 2.7 GHz up to and including 2.9 GHz;

b.4.a.2. A peak saturated power output greater than 270 W (54.3 dBm) at any frequency exceeding 2.9 GHz up to and including 3.2 GHz;

b.4.a.3. A peak saturated power output greater than 200 W (53 dBm) at any frequency exceeding 3.2 GHz up to and including 3.7 GHz; or

b.4.a.4. A peak saturated power output greater than 90 W (49.54 dBm) at any frequency exceeding 3.7 GHz up to and including 6.8 GHz;

b.4.b. Rated for operation at frequencies exceeding 6.8 GHz up to and including 31.8 GHz with a “fractional bandwidth” greater than 10%, and having any of the following:

b.4.b.1. A peak saturated power output greater than 70 W (48.45 dBm) at any frequency exceeding 6.8 GHz up to and including 8.5 GHz;

b.4.b.2. A peak saturated power output greater than 50 W (47 dBm) at any frequency exceeding 8.5 GHz up to and including 12 GHz;

b.4.b.3. A peak saturated power output greater than 30 W (44.77 dBm) at any frequency exceeding 12 GHz up to and including 16 GHz; or

b.4.b.4. A peak saturated power output greater than 20 W (43 dBm) at any frequency exceeding 16 GHz up to and including 31.8 GHz;

b.4.c. Rated for operation with a peak saturated power output greater than 0.5 W (27 dBm) at any frequency exceeding 31.8 GHz up to and including 37 GHz;

b.4.d. Rated for operation with a peak saturated power output greater than 2 W (33 dBm) at any frequency exceeding 37 GHz up to and including 43.5 GHz, and with a “fractional bandwidth” of greater than 10%;

b.4.e. Rated for operation at frequencies exceeding 43.5 GHz and having any of the following:

b.4.e.1. A peak saturated power output greater than 0.2 W (23 dBm) at any frequency exceeding 43.5 GHz up to and including 75 GHz, and with a “fractional bandwidth” of greater than 10%;

b.4.e.2. A peak saturated power output greater than 20 mW (13 dBm) at any frequency exceeding 75 GHz up to and including 90 GHz, and with a “fractional bandwidth” of greater than 5%; or

b.4.e.3. A peak saturated power output greater than 0.1 nW (-70 dBm) at any frequency exceeding 90 GHz; or

b.4.f. [Reserved]

N.B.:

1. For “MMIC” amplifiers see 3A001.b.2.

2. For ‘transmit/receive modules’ and ‘transmit modules’ see 3A001.b.12.

3. For converters and harmonic mixers, designed to extend the operating or frequency range of signal analyzers, signal generators, network analyzers or microwave test receivers, see 3A001.b.7.

Note 1: [Reserved]

Note 2: *The control status of an item whose rated operating frequency includes frequencies listed in more than one frequency range, as defined by 3A001.b.4.a through 3A001.b.4.e, is determined by the lowest peak saturated power output control threshold.*

b.5. Electronically or magnetically tunable band-pass or band-stop filters, having more than 5 tunable resonators capable of tuning across a 1.5:1 frequency band (f_{\max}/f_{\min}) in less than 10 ms and having any of the following:

b.5.a. A band-pass bandwidth of more than 0.5% of center frequency; or

b.5.b. A band-stop bandwidth of less than 0.5% of center frequency;

b.6. [Reserved]

b.7. Converters and harmonic mixers, that are any of the following:

b.7.a. Designed to extend the frequency range of “signal analyzers” beyond 90 GHz;

b.7.b. Designed to extend the operating range of signal generators as follows:

b.7.b.1. Beyond 90 GHz;

b.7.b.2. To an output power greater than 100 mW (20 dBm) anywhere within the frequency range exceeding 43.5 GHz but not exceeding 90 GHz;

b.7.c. Designed to extend the operating range of network analyzers as follows:

b.7.c.1. Beyond 110 GHz;

b.7.c.2. To an output power greater than 31.62 mW (15 dBm) anywhere within the frequency range exceeding 43.5 GHz but not exceeding 90 GHz;

b.7.c.3. To an output power greater than 1 mW (0 dBm) anywhere within the frequency range exceeding 90 GHz but not exceeding 110 GHz; or

b.7.d. Designed to extend the frequency range of microwave test receivers beyond 110 GHz;

b.8. Microwave power amplifiers containing “vacuum electronic devices” controlled by 3A001.b.1 and having all of the following:

b.8.a. Operating frequencies above 3 GHz;

b.8.b. An average output power to mass ratio exceeding 80 W/kg; and

b.8.c. A volume of less than 400 cm³;

Note: *3A001.b.8 does not control equipment designed or rated for operation in any frequency band which is “allocated by the ITU” for radio-communications services, but not for radio-determination.*

b.9. Microwave Power Modules (MPM) consisting of, at least, a traveling-wave “vacuum electronic device,” a “Monolithic Microwave Integrated Circuit” (“MMIC”) and an integrated electronic power conditioner and having all of the following:

b.9.a. A “turn-on time” from off to fully operational in less than 10 seconds;

b.9.b. A volume less than the maximum rated power in Watts multiplied by 10 cm³/W; and

b.9.c. An “instantaneous bandwidth” greater than 1 octave ($f_{\max} > 2f_{\min}$) and having any of the following:

b.9.c.1. For frequencies equal to or less than 18 GHz, an RF output power greater than 100 W; or

b.9.c.2. A frequency greater than 18 GHz;

Technical Notes: *For the purposes of 3A001.b.9:*

1. *To calculate the volume in 3A001.b.9.b, the following example is provided: for a maximum rated power of 20 W, the volume would be: $20 \text{ W} \times 10 \text{ cm}^3/\text{W} = 200 \text{ cm}^3$.*

2. *The ‘turn-on time’ in 3A001.b.9.a refers to the time from fully-off to fully operational, i.e., it includes the warm-up time of the MPM.*

b.10. Oscillators or oscillator assemblies, specified to operate with a single sideband (SSB) phase noise, in dBc/Hz, less (better) than $-(126 + 20\log_{10}F - 20\log_{10}f)$ anywhere within the range of 10 Hz $\leq f \leq 10$ kHz;

Technical Note: *For the purposes of 3A001.b.10, F is the offset from the operating frequency in Hz and f is the operating frequency in MHz.*

b.11. ‘Frequency synthesizer’ “electronic assemblies” having a “frequency switching time” as specified by any of the following:

b.11.a. Less than 143 ps;

b.11.b. Less than 100 μ s for any frequency change exceeding 2.2 GHz within the synthesized frequency range exceeding 4.8 GHz but not exceeding 31.8 GHz;

b.11.c. [Reserved]

b.11.d. Less than 500 μ s for any frequency change exceeding 550 MHz within the synthesized frequency range exceeding 31.8 GHz but not exceeding 37 GHz;

b.11.e. Less than 100 μ s for any frequency change exceeding 2.2 GHz within the synthesized frequency range exceeding 37 GHz but not exceeding 75 GHz;

b.11.f. Less than 100 μ s for any frequency change exceeding 5.0 GHz within the synthesized frequency range exceeding 75 GHz but not exceeding 90 GHz; or

b.11.g. Less than 1 ms within the synthesized frequency range exceeding 90 GHz;

Technical Note: *For the purposes of 3A001.b.11, a ‘frequency synthesizer’ is any kind of frequency source, regardless of the actual technique used, providing a multiplicity of simultaneous or alternative output frequencies, from one or more outputs, controlled by, derived from or disciplined by a lesser number of standard (or master) frequencies.*

N.B.: For general purpose “signal analyzers”, signal generators, network analyzers and microwave test receivers, see 3A002.c, 3A002.d, 3A002.e and 3A002.f, respectively.

b.12. ‘Transmit/receive modules,’ ‘transmit/receive MMICs,’ ‘transmit modules,’ and ‘transmit MMICs,’ rated for operation at frequencies above 2.7 GHz and having all of the following:

b.12.a. A peak saturated power output (in watts), P_{sat} , greater than 505.62 divided by the maximum operating frequency (in GHz) squared [$P_{\text{sat}} > 505.62 \text{ W} * \text{GHz}^2 / f_{\text{GHz}}^2$] for any channel;

b.12.b. A “fractional bandwidth” of 5% or greater for any channel;

b.12.c. Any planar side with length d (in cm) equal to or less than 15 divided by the lowest operating frequency in GHz [$d \leq 15 \text{ cm} * \text{GHz} * N / f_{\text{GHz}}$] where N is the number of transmit or transmit/receive channels; and

b.12.d. An electronically variable phase shifter per channel.

Technical Notes: For the purposes of 3A001.b.12:

1. A ‘transmit/receive module’ is a multifunction “electronic assembly” that provides bi-directional amplitude and phase control for transmission and reception of signals.

2. A ‘transmit module’ is an “electronic assembly” that provides amplitude and phase control for transmission of signals.

3. A ‘transmit/receive MMIC’ is a multifunction “MMIC” that provides bi-directional amplitude and phase control for transmission and reception of signals.

4. A ‘transmit MMIC’ is a “MMIC” that provides amplitude and phase control for transmission of signals.

5. 2.7 GHz should be used as the lowest operating frequency (f_{GHz}) in the formula in 3A001.b.12.c for transmit/receive or transmit modules that have a rated operation range extending downward to 2.7 GHz and below [$d \leq 15 \text{ cm} * \text{GHz} * N / 2.7 \text{ GHz}$].

6. 3A001.b.12 applies to ‘transmit/receive modules’ or ‘transmit modules’ with or without a heat sink. The value of d in 3A001.b.12.c does not include any portion of the ‘transmit/receive module’ or ‘transmit module’ that functions as a heat sink.

7. ‘Transmit/receive modules,’ ‘transmit modules,’ ‘transmit/receive MMICs’ or ‘transmit MMICs’ may or may not have N integrated radiating antenna elements where N is the number of transmit or transmit/receive channels.

c. Acoustic wave devices as follows and “specially designed” “components” therefor:

c.1. Surface acoustic wave and surface skimming (shallow bulk) acoustic wave devices, having any of the following:

c.1.a. A carrier frequency exceeding 6 GHz;

c.1.b. A carrier frequency exceeding 1 GHz, but not exceeding 6 GHz and having any of the following:

c.1.b.1. A ‘frequency side-lobe rejection’ exceeding 65 dB;

c.1.b.2. A product of the maximum delay time and the bandwidth (time in μs and bandwidth in MHz) of more than 100;

c.1.b.3. A bandwidth greater than 250 MHz; or

c.1.b.4. A dispersive delay of more than 10 μs ; or

c.1.c. A carrier frequency of 1 GHz or less and having any of the following:

c.1.c.1. A product of the maximum delay time and the bandwidth (time in μs and bandwidth in MHz) of more than 100;

c.1.c.2. A dispersive delay of more than 10 μs ; or

c.1.c.3. A ‘frequency side-lobe rejection’ exceeding 65 dB and a bandwidth greater than 100 MHz;

Technical Note: For the purposes of 3A001.c.1, ‘frequency side-lobe rejection’ is the maximum rejection value specified in data sheet.

c.2. Bulk (volume) acoustic wave devices that permit the direct processing of signals at frequencies exceeding 6 GHz;

c.3. Acoustic-optic “signal processing” devices employing interaction between acoustic waves (bulk wave or surface wave) and light waves that permit the direct processing of signals or images, including spectral analysis, correlation or convolution;

Note: 3A001.c does not control acoustic wave devices that are limited to a single band pass, low pass, high pass or notch filtering, or resonating function.

d. Electronic devices and circuits containing “components,” manufactured from “superconductive” materials, “specially designed” for operation at temperatures below the “critical temperature” of at least one of the “superconductive” constituents and having any of the following:

d.1. Current switching for digital circuits using “superconductive” gates with a product of delay time per gate (in seconds) and power dissipation per gate (in watts) of less than 10^{-14} J; or

d.2. Frequency selection at all frequencies using resonant circuits with Q-values exceeding 10,000;

e. High energy devices as follows:

e.1. ‘Cells’ as follows:

e.1.a. ‘Primary cells’ having any of the following at 20 °C:

e.1.a.1. ‘Energy density’ exceeding 550 Wh/kg and a ‘continuous power density’ exceeding 50 W/kg; or

e.1.a.2. ‘Energy density’ exceeding 50 Wh/kg and a ‘continuous power density’ exceeding 350 W/kg;

e.1.b. ‘Secondary cells’ having an ‘energy density’ exceeding 350 Wh/kg at 20 °C;

Technical Notes:

1. For the purposes of 3A001.e.1, ‘energy density’ (Wh/kg) is calculated from the nominal voltage multiplied by the nominal capacity in ampere-hours (Ah) divided by the mass in kilograms. If the nominal capacity is not stated, energy density is calculated from the nominal voltage squared then multiplied by the discharge duration in hours divided by the discharge load in Ohms and the mass in kilograms.

2. For the purposes of 3A001.e.1, a ‘cell’ is defined as an electrochemical device, which has positive and negative electrodes, an electrolyte, and is a source of electrical energy. It is the basic building block of a battery.

3. For the purposes of 3A001.e.1.a, a ‘primary cell’ is a ‘cell’ that is not designed to be charged by any other source.

4. For the purposes of 3A001.e.1.b, a ‘secondary cell’ is a ‘cell’ that is designed to be charged by an external electrical source.

5. For the purposes of 3A001.e.1.a, ‘continuous power density’ (W/kg) is calculated from the nominal voltage multiplied by the specified maximum continuous discharge current in ampere (A) divided by the mass in kilograms. ‘Continuous power density’ is also referred to as specific power.

Note: 3A001.e does not control batteries, including single-cell batteries.

e.2. High energy storage capacitors as follows:

e.2.a. Capacitors with a repetition rate of less than 10 Hz (single shot capacitors) and having all of the following:

e.2.a.1. A voltage rating equal to or more than 5 kV;

e.2.a.2. An energy density equal to or more than 250 J/kg; and

e.2.a.3. A total energy equal to or more than 25 kJ;

e.2.b. Capacitors with a repetition rate of 10 Hz or more (repetition rated capacitors) and having all of the following:

e.2.b.1. A voltage rating equal to or more than 5 kV;

e.2.b.2. An energy density equal to or more than 50 J/kg;

e.2.b.3. A total energy equal to or more than 100 J; and

e.2.b.4. A charge/discharge cycle life equal to or more than 10,000;

e.3. “Superconductive” electromagnets and solenoids, “specially designed” to be fully charged or discharged in less than one second and having all of the following:

Note: 3A001.e.3 does not control “superconductive” electromagnets or solenoids “specially designed” for Magnetic Resonance Imaging (MRI) medical equipment.

e.3.a. Energy delivered during the discharge exceeding 10 kJ in the first second;

e.3.b. Inner diameter of the current carrying windings of more than 250 mm; and

e.3.c. Rated for a magnetic induction of more than 8 T or “overall current density” in the winding of more than 300 A/mm²;

e.4. Solar cells, cell-interconnect-coverglass (CIC) assemblies, solar panels, and solar arrays, which are “space-qualified,” having a minimum average efficiency exceeding 20% at an operating temperature of 301 K (28 °C) under simulated ‘AM0’ illumination with an irradiance of 1,367 Watts per square meter (W/m²);

Technical Note: For the purposes of 3A001.e.4, ‘AM0’, or ‘Air Mass Zero’, refers to the spectral irradiance of sun light in the earth’s outer atmosphere when the distance between the earth and sun is one astronomical unit (AU).

f. Rotary input type absolute position encoders having an “accuracy” equal to or less (better) than 1.0 second of arc and “specially designed” encoder rings, discs or scales therefor;

g. Solid-state pulsed power switching thyristor devices and ‘thyristor modules’, using either electrically, optically, or electron radiation controlled switch methods and having any of the following:

g.1. A maximum turn-on current rate of rise (di/dt) greater than 30,000 A/ μs and off-state voltage greater than 1,100 V; or

g.2. A maximum turn-on current rate of rise (di/dt) greater than 2,000 A/μs and having all of the following:

g.2.a. An off-state peak voltage equal to or greater than 3,000 V; and

g.2.b. A peak (surge) current equal to or greater than 3,000 A;

Note 1: 3A001.g. includes:

- Silicon Controlled Rectifiers (SCRs)
- Electrical Triggering Thyristors (ETTs)
- Light Triggering Thyristors (LTTs)
- Integrated Gate Commutated Thyristors (IGCTs)
- Gate Turn-off Thyristors (GTOs)
- MOS Controlled Thyristors (MCTs)
- Solidtrons

Note 2: 3A001.g does not control thyristor devices and ‘thyristor modules’ incorporated into equipment designed for civil railway or “civil aircraft” applications.

Technical Note: For the purposes of 3A001.g, a ‘thyristor module’ contains one or more thyristor devices.

h. Solid-state power semiconductor switches, diodes, or ‘modules’, having all of the following:

h.1. Rated for a maximum operating junction temperature greater than 488 K (215 °C);

h.2. Repetitive peak off-state voltage (blocking voltage) exceeding 300 V; and

h.3. Continuous current greater than 1 A.

Technical Note: For the purposes of 3A001.h, ‘modules’ contain one or more solid-state power semiconductor switches or diodes.

Note 1: Repetitive peak off-state voltage in 3A001.h includes drain to source voltage, collector to emitter voltage, repetitive peak reverse voltage and peak repetitive off-state blocking voltage.

Note 2: 3A001.h includes:

- Junction Field Effect Transistors (JFETs)
- Vertical Junction Field Effect Transistors (VFETs)
- Metal Oxide Semiconductor Field Effect Transistors (MOSFETs)
- Double Diffused Metal Oxide Semiconductor Field Effect Transistor (DMOSFET)
- Insulated Gate Bipolar Transistor (IGBT)
- High Electron Mobility Transistors (HEMTs)
- Bipolar Junction Transistors (BJTs)
- Thyristors and Silicon Controlled Rectifiers (SCRs)
- Gate Turn-Off Thyristors (GTOs)
- Emitter Turn-Off Thyristors (ETOs)
- PiN Diodes
- Schottky Diodes

Note 3: 3A001.h does not apply to switches, diodes, or ‘modules’, incorporated into equipment designed for civil automobile, civil railway, or “civil aircraft” applications.

i. Intensity, amplitude, or phase electro-optic modulators, designed for analog signals and having any of the following:

i.1. A maximum operating frequency of more than 10 GHz but less than 20 GHz, an optical insertion loss equal to or less than 3 dB and having any of the following:

i.1.a. A ‘half-wave voltage’ (‘Vπ’) less than 2.7 V when measured at a frequency of 1 GHz or below; or

i.1.b. A ‘Vπ’ of less than 4 V when measured at a frequency of more than 1 GHz; or

i.2. A maximum operating frequency equal to or greater than 20 GHz, an optical insertion loss equal to or less than 3 dB and having any of the following:

i.2.a. A ‘Vπ’ less than 3.3 V when measured at a frequency of 1 GHz or below; or

i.2.b. A ‘Vπ’ less than 5 V when measured at a frequency of more than 1 GHz.

Note: 3A001.i includes electro-optic modulators having optical input and output connectors (e.g., fiber-optic pigtails).

Technical Note: For the purposes of 3A001.i, a ‘half-wave voltage’ (‘Vπ’) is the applied voltage necessary to make a phase change of 180 degrees in the wavelength of light propagating through the optical modulator.

j. through y. [Reserved]

z. Any commodity described in 3A001 that meets or exceeds the performance parameters in 3A090, as follows:

z.1. “Monolithic Microwave Integrated Circuit” (“MMIC”) amplifiers described in 3A001.b.2 and discrete microwave transistors in 3A001.b.3 that also meet or exceed the performance parameters in ECCN 3A090, except those 3A001.b.2 and b.3 items being exported or reexported for use in civil telecommunications applications;

z.2. Commodities that are described in 3A001.a.1.a when usable in “missiles” that also meet or exceed the performance parameters in ECCN 3A090; and to 3A001.a.5.a when “designed or modified” for military use, hermetically sealed and rated for operation in the temperature range from below –54 °C to above +125 °C and that also meet or exceed the performance parameters in ECCN 3A090;

z.3. Pulse discharge capacitors described in 3A001.e.2 and superconducting solenoidal electromagnets in 3A001.e.3 that meet or exceed the technical parameters in 3A201.a and 3A201.b, respectively and that also meet or exceed the performance parameters in ECCN 3A090; or

z.4. All other commodities specified in this ECCN that meet or exceed the performance parameters of ECCN 3A090.

* * * * *

3A090 Integrated circuits as follows (see List of Items Controlled).

License Requirements

Reason for Control: RS, AT

Control(s)	Country Chart (see Supp. No. 1 to part 738)
RS applies to entire entry.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.

Control(s)	Country Chart (see Supp. No. 1 to part 738)
AT applies to entire entry.	AT Column 1.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

LVS: N/A

GBS: N/A

NAC/ACA: Yes, for 3A090.a, if the item is not designed or marketed for use in datacenters and has a ‘total processing performance’ of 4800 or more; yes, for 3A090.b, if the item is designed or marketed for use in datacenters.

List of Items Controlled

Related Controls: (1) See ECCNs 3D001, 3E001, 5D002.z, and 5D992.z for associated technology and software controls. (2) See ECCNs 3A001.z, 5A002.z, 5A004.z, and 5A992.z.

Related Definitions: N/A

Items:

a. Integrated circuits having one or more digital processing units having either of the following:

a.1. A ‘total processing performance’ of 4800 or more, or

a.2. A ‘total processing performance’ of 1600 or more and a ‘performance density’ of 5.92 or more.

b. Integrated circuits having one or more digital processing units having either of the following:

b.1. A ‘total processing performance’ of 2400 or more and less than 4800 and a ‘performance density’ of 1.6 or more and less than 5.92, or

b.2. A ‘total processing performance’ of 1600 or more and a ‘performance density’ of 3.2 or more and less than 5.92.

Note 1 to 3A090: Integrated circuits specified by 3A090 include graphical processing units (GPUs), tensor processing units (TPUs), neural processors, in-memory processors, vision processors, text processors, co-processors/accelerators, adaptive processors, field-programmable logic devices (FPLDs), and application-specific integrated circuits (ASICs). Examples of integrated circuits are in the Note to 3A001.a.

Note 2 to 3A090: 3A090 does not apply to items that are not designed or marketed for use in datacenters and do not have a ‘total processing performance’ of 4800 or more. For integrated circuits that are not designed or marketed for use in datacenters and that have a ‘total processing performance’ of 4800 or more, see license exceptions NAC and ACA.

Note 3 to 3A090: For ICs that are excluded from ECCN 3A090 under Note 2 or 3 to 3A090, those ICs are also not applicable for classifications made under ECCNs 3A001.z, 4A003.z, 4A004.z, 4A005.z, 4A090, 5A002.z, 5A004.z, 5A992.z, 5D002.z, or 5D992.z because those other CCL classifications are based on the incorporation of an IC that meets the control parameters under ECCN 3A090 or otherwise meets or exceeds the control parameters or ECCNs 3A090 or 4A090. See the Related Controls paragraphs of 3A001.z, 4A003.z, 4A004.z, 4A005.z,

4A090, 5A002.z, 5A004.z, 5A992.z, 5D002.z, or 5D992.z.

Technical Notes:

1. 'Total processing performance' ('TPP') is $2 \times \text{MacTOPS} \times \text{'bit length of the operation'}$, aggregated over all processing units on the integrated circuit.

a. For purposes of 3A090, 'MacTOPS' is the theoretical peak number of Tera (10^{12}) operations per second for multiply-accumulate computation ($D = A \times B + C$).

b. The 2 in the 'TPP' formula is based on industry convention of counting one multiply-accumulate computation, $D = A \times B + C$, as 2 operations for purpose of datasheets. Therefore, $2 \times \text{MacTOPS}$ may correspond to the reported TOPS or FLOPS on a datasheet.

c. For purposes of 3A090, 'bit length of the operation' for a multiply-accumulate computation is the largest bit-length of the inputs to the multiply operation.

d. Aggregate the TPPs for each processing unit on the integrated circuit to arrive at a total. $\text{TPP} = \text{TPP}_1 + \text{TPP}_2 + \dots + \text{TPP}_n$ (where n is the number of processing units on the integrated circuit).

2. The rate of 'MacTOPS' is to be calculated at its maximum value theoretically possible. The rate of 'MacTOPS' is assumed to be the highest value the manufacturer claims in annual or brochure for the integrated circuit. For example, the 'TPP' threshold of 4800 can be met with 600 tera integer operations (or 2×300 'MacTOPS') at 8 bits or 300 tera FLOPS (or 2×150 'MacTOPS') at 16 bits. If the IC is designed for MAC computation with multiple bit lengths that achieve different 'TPP' values, the highest 'TPP' value should be evaluated against parameters in 3A090.

3. For integrated circuits specified by 3A090 that provide processing of both sparse and dense matrices, the 'TPP' values are the values for processing of dense matrices (e.g., without sparsity).

4. 'Performance density' is 'TPP' divided by 'applicable die area'. For purposes of 3A090, 'applicable die area' is measured in millimeters squared and includes all die area of logic dies manufactured with a process node that uses a non-planar transistor architecture.

* * * * *

3B001 Equipment for the manufacturing of semiconductor devices, materials, or related equipment, as follows (see List of Items Controlled) and "specially designed" "components" and "accessories" therefor.

License Requirements

Reason for Control: NS, RS, AT

Control(s)	Country chart (see Supp. No. 1 to part 738)
NS applies to 3B001.a.1 to a.3, b, e, f.1.a, f.2 to f.4, g to i.	NS Column 2.

Control(s)	Country chart (see Supp. No. 1 to part 738)
NS applies to 3B001.a.4, c, d, f.1.b, j to p.	To or within Macau or a destination specified in Country Group D:5 of supplement no. 1 to part 740 of the EAR. See § 742.4(a)(4) of the EAR.
RS applies to 3B001.a.4, c, d, f.1.b, j to p.	To or within Macau or a destination specified in Country Group D:5 of supplement no. 1 to part 740 of the EAR. See § 742.6(a)(6) of the EAR.
AT applies to entire entry.	AT Column 1.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

LVS: \$500, except semiconductor manufacturing equipment specified in 3B001.a.4, c, d, f.1.b, j to p.

GBS: Yes, except a.3 (molecular beam epitaxial growth equipment using gas sources), .e (automatic loading multi-chamber central wafer handling systems only if connected to equipment controlled by 3B001.a.3, or .f), and .f (lithography equipment).

List of Items Controlled

Related Controls: See also 3B991

Related Definitions: N/A
Items:

a. Equipment designed for epitaxial growth as follows:

a.1. Equipment designed or modified to produce a layer of any material other than silicon with a thickness uniform to less than $\pm 2.5\%$ across a distance of 75 mm or more;

Note: 3B001.a.1 includes atomic layer epitaxy (ALE) equipment.

a.2. Metal Organic Chemical Vapor Deposition (MOCVD) reactors designed for compound semiconductor epitaxial growth of material having two or more of the following elements: aluminum, gallium, indium, arsenic, phosphorus, antimony, or nitrogen;

a.3. Molecular beam epitaxial growth equipment using gas or solid sources;

a.4. Equipment designed for silicon (Si), carbon doped silicon, silicon germanium (SiGe), or carbon doped SiGe epitaxial growth, and having all of the following:

a.4.a. Multiple chambers and maintaining high vacuum (equal to or less than 0.01 Pa) or inert environment (water and oxygen partial pressure less than 0.01 Pa) between process steps;

a.4.b. At least one preclean chamber designed to provide a surface preparation means to clean the surface of the wafer; and
a.4.c. An epitaxial deposition operating temperature of 685 °C or below;

b. Semiconductor wafer fabrication equipment designed for ion implantation and having any of the following:

b.1. [Reserved]

b.2. Being designed and optimized to operate at a beam energy of 20 keV or more and a beam current of 10 mA or more for hydrogen, deuterium, or helium implant;

b.3. Direct write capability;

b.4. A beam energy of 65 keV or more and a beam current of 45 mA or more for high energy oxygen implant into a heated semiconductor material "substrate"; or

b.5. Being designed and optimized to operate at beam energy of 20 keV or more and a beam current of 10 mA or more for silicon implant into a semiconductor material "substrate" heated to 600 °C or greater;

c. Etch equipment.
c.1. Equipment designed for dry etching as follows:

c.1.a. Equipment designed or modified for isotropic dry etching, having a largest 'silicon germanium-to-silicon (SiGe:Si) etch selectivity' of greater than or equal to 100:1; or

c.1.b. Equipment designed or modified for anisotropic etching of dielectric materials and enabling the fabrication of high aspect ratio features with aspect ratio greater than 30:1 and a lateral dimension on the top surface of less than 100 nm, and having all of the following:

c.1.b.1. Radio Frequency (RF) power source(s) with at least one pulsed RF output; and

c.1.b.2. One or more fast gas switching valve(s) with switching time less than 300 milliseconds; or

c.1.c. Equipment designed or modified for anisotropic dry etching, having all of the following:

c.1.c.1. Radio Frequency (RF) power source(s) with at least one pulsed RF output;

c.1.c.2. One or more fast gas switching valve(s) with switching time less than 300 milliseconds; and

c.1.c.3. Electrostatic chuck with twenty or more individually controllable variable temperature elements;

c.2. Equipment designed for wet chemical processing and having a largest 'silicon germanium-to-silicon (SiGe:Si) etch selectivity' of greater than or equal to 100:1;

Note 1: 3B001.c includes etching by 'radicals', ions, sequential reactions, or non-sequential reaction.

Note 2: 3B001.c.1.c includes etching using RF pulse excited plasma, pulsed duty cycle excited plasma, pulsed voltage on electrodes modified plasma, cyclic injection and purging of gases combined with a plasma, plasma atomic layer etching, or plasma quasi-atomic layer etching.

Technical Notes:

1. For the purposes of 3B001.c, 'silicon germanium-to-silicon (SiGe:Si) etch selectivity' is measured for a Ge concentration of greater than or equal to 30% (Si_{0.70}Ge_{0.30}).

2. For the purposes of 3B001.c Note 1 and 3B001.d.14, 'radical' is defined as an atom, molecule, or ion that has an unpaired electron in an open electron shell configuration.

d. Semiconductor manufacturing deposition equipment, as follows:

d.1. Equipment designed for cobalt (Co) electroplating or cobalt electroless-plating deposition processes;

Note: 3B001.d.1 controls semiconductor wafer processing equipment.

d.2. Equipment designed for:

d.2.a. Chemical vapor deposition of cobalt (Co) fill metal; or

d.2.b. Selective bottom-up chemical vapor deposition of tungsten (W) fill metal;

d.3. Equipment designed to fabricate a metal contact by multistep processing within a single chamber by performing all of the following:

d.3.a. Deposition of a tungsten layer, using an organometallic compound, while maintaining the wafer substrate temperature greater than 100 °C and less than 500 °C; and

d.3.b. A plasma process using hydrogen (H₂), including hydrogen and nitrogen (H₂ + N₂) or ammonia (NH₃);

d.4. Equipment or systems designed for multistep processing in multiple chambers or stations and maintaining high vacuum (equal to or less than 0.01 Pa) or inert environment between process steps, as follows:

d.4.a. Equipment designed to fabricate a metal contact by performing the following processes:

d.4.a.1. Surface treatment plasma process using hydrogen (H₂), including hydrogen and nitrogen (H₂ + N₂) or ammonia (NH₃), while maintaining the wafer substrate at a temperature greater than 100 °C and less than 500 °C;

d.4.a.2. Surface treatment plasma process using oxygen (O₂) or ozone (O₃), while maintaining the wafer substrate at a temperature greater than 40 °C and less than 500 °C; and

d.4.a.3. Deposition of a tungsten layer while maintaining the wafer substrate temperature greater than 100 °C and less than 500 °C;

d.4.b. Equipment designed to fabricate a metal contact by performing the following processes:

d.4.b.1. Surface treatment process using a remote plasma generator and an ion filter; and

d.4.b.2. Deposition of a cobalt (Co) layer selectively onto copper (Cu) using an organometallic compound;

Note: This control does not apply to equipment that is non-selective.

d.4.c. Equipment designed to fabricate a metal contact by performing all the following processes:

d.4.c.1. Deposition of a titanium nitride (TiN) or tungsten carbide (WC) layer, using an organometallic compound, while maintaining the wafer substrate at a temperature greater than 20 °C and less than 500 °C;

d.4.c.2. Deposition of a cobalt (Co) layer using a physical sputter deposition technique and having a process pressure greater than 133.3 mPa and less than 13.33 Pa, while maintaining the wafer substrate at a temperature below 500 °C; and

d.4.c.3. Deposition of a cobalt (Co) layer using an organometallic compound and having a process pressure greater than 133.3 Pa and less than 13.33 kPa, while maintaining the wafer substrate at a temperature greater than 20 °C and less than 500 °C;

d.4.d. Equipment designed to fabricate copper (Cu) interconnects by performing all of the following processes:

d.4.d.1. Deposition of a cobalt (Co) or ruthenium (Ru) layer using an organometallic compound and having a process pressure greater than 133.3 Pa and less than 13.33 kPa, while maintaining the wafer substrate at a temperature greater than 20 °C and less than 500 °C; and

d.4.d.2. Deposition of a copper layer using a physical vapor deposition technique and having a process pressure greater than 133.3 mPa and less than 13.33 Pa, while maintaining the wafer substrate at a temperature below 500 °C;

d.5. Equipment designed for plasma enhanced chemical vapor deposition of carbon hard masks more than 100 nm thick and with stress less than 450 MPa;

d.6. Atomic Layer Deposition (ALD) equipment designed for area selective deposition of a barrier or liner using an organometallic compound;

Note: 3B001.d.6 includes equipment capable of area selective deposition of a barrier layer to enable fill metal contact to an underlying electrical conductor without a barrier layer at the fill metal via interface to an underlying electrical conductor.

d.7. Equipment designed for Atomic Layer Deposition (ALD) of tungsten (W) to fill an entire interconnect or in a channel less than 40 nm wide, while maintaining the wafer substrate at a temperature less than 500 °C.

d.8. Equipment designed for Atomic Layer Deposition (ALD) of 'work function metal' having all of the following:

d.8.a. More than one metal source of which one is designed for an aluminum (Al) precursor;

d.8.b. Precursor vessel designed and enabled to operate at a temperature greater than 30 °C; and

d.8.c. Designed for depositing a 'work function metal' having all of the following:

d.8.c.1. Deposition of titanium-aluminum carbide (TiAlC); and

d.8.c.2. Enabling a work function greater than 4.0eV;

Technical Note: For the purposes of 3B001.d.8, 'work function metal' is a material that controls the threshold voltage of a transistor.

d.9. Spatial Atomic Layer Deposition (ALD) equipment having a wafer support platform that rotates around an axis having any of the following:

d.9.a. A spatial plasma enhanced atomic layer deposition mode of operation;

d.9.b. A plasma source; or

d.9.c. A plasma shield or means to confine the plasma to the plasma exposure process region;

d.10. Equipment designed for Atomic Layer Deposition (ALD) or Chemical Vapor Deposition (CVD) of plasma enhanced of low fluorine tungsten (FW) (fluorine (F) concentration less than 10¹⁹ atoms/cm³) films;

d.11. Equipment designed to deposit a metal layer, in a vacuum (equal to or less than 0.01 Pa) or inert gas environment, and having all of the following:

d.11.a. A Chemical Vapor Deposition (CVD) or cyclic deposition process for depositing a tungsten nitride (WN) layer, while maintaining the wafer substrate at a temperature greater than 20 °C and less than 500 °C; and

d.11.b. A Chemical Vapor Deposition (CVD) or cyclic deposition process for depositing a tungsten (W) layer having a process pressure greater than 133.3 Pa and less than 53.33 kPa, while maintaining the wafer substrate at a temperature greater than 20 °C and less than 500 °C.

d.12. Equipment designed for depositing a metal layer, in a vacuum (equal to or less than 0.01 Pa) or inert gas environment, and having any of the following:

d.12.a. Selective tungsten (W) growth without a barrier; or

d.12.b. Selective molybdenum (Mo) growth without a barrier;

d.13. Equipment designed for depositing a ruthenium layer (Ru) using an organometallic compound, while maintaining the wafer substrate at a temperature greater than 20 °C and less than 500 °C;

d.14. Equipment designed for deposition assisted by remotely generated 'radicals', enabling the fabrication of a silicon (Si) and carbon (C) containing film, and having all of the following properties of the deposited film:

d.14.a. A dielectric constant (k) of less than 5.3;

d.14.b. An aspect ratio greater than 5:1 in features with lateral openings of less than 70 nm; and

d.14.c. A feature-to-feature pitch of less than 100 nm;

d.15. Equipment designed for void free plasma enhanced deposition of a low-k dielectric layer in gaps between metal lines less than 25 nm and having an aspect ratio greater than or equal to 1:1 with a less than 3.3 dielectric constant;

d.16. Equipment designed for deposition of a film, containing silicon and carbon, and having a dielectric constant (k) of less than 5.3, into lateral openings having widths of less than 70 nm and aspect ratios greater than 5:1 (depth: width) and a feature-to-feature pitch of less than 100 nm, while maintaining the wafer substrate at a temperature greater than 400 °C and less than 650 °C, and having all of the following:

d.16.a. Boat designed to hold multiple vertically stacked wafers;

d.16.b. Two or more vertical injectors; and

d.16.c. A silicon source and propene are introduced to a different injector than a nitrogen source or an oxygen source;

e. Automatic loading multi-chamber central wafer handling systems having all of the following:

e.1. Interfaces for wafer input and output, to which more than two functionally different 'semiconductor process tools'

controlled by 3B001.a.1, 3B001.a.2, 3B001.a.3 or 3B001.b are designed to be connected; and

e.2. Designed to form an integrated system in a vacuum environment for 'sequential multiple wafer processing';

Note: 3B001.e does not control automatic robotic wafer handling systems "specially designed" for parallel wafer processing.

Technical Notes:

1. For the purposes of 3B001.e, 'semiconductor process tools' refers to modular tools that provide physical processes for semiconductor production that are functionally different, such as deposition, implant or thermal processing.

2. For the purposes of 3B001.e, 'sequential multiple wafer processing' means the capability to process each wafer in different 'semiconductor process tools', such as by transferring each wafer from one tool to a second tool and on to a third tool with the automatic loading multi-chamber central wafer handling systems.

f. Lithography equipment as follows:
 f.1. Align and expose step and repeat (direct step on wafer) or step and scan (scanner) equipment for wafer processing using photo-optical or X-ray methods and having any of the following:

f.1.a. A light source wavelength shorter than 193 nm; or
 f.1.b. A light source wavelength equal to or longer than 193 nm and having all of the following:

f.1.b.1. The capability to produce a pattern with a "Minimum Resolvable Feature size" (MRF) of 45 nm or less; and

f.1.b.2. Having any of the following:

f.1.b.2.a. A maximum 'dedicated chuck overlay' value of less than or equal to 1.50 nm; or

f.1.b.2.b. A maximum 'dedicated chuck overlay' value greater than 1.50 nm but less than or equal to 2.40 nm;

Technical Notes: For the purposes of 3B001.f.1.b:

1. The 'Minimum Resolvable Feature size' (MRF), i.e., resolution, is calculated by the following formula:

(an exposure light source wavelength in nm) x (K factor)

MRF = -----

maximum numerical aperture

where, for the purposes of 3.B.1.f.1.b, the K factor = 0.25 'MRF' is also known as resolution.

2. 'Dedicated chuck overlay' is the alignment accuracy of a new pattern to an existing pattern printed on a wafer by the same lithographic system. 'Dedicated chuck overlay' is also known as single machine overlay.

f.2. Imprint lithography equipment capable of production features of 45 nm or less;

Note: 3B001.f.2 includes:

- Micro contact printing tools
- Hot embossing tools
- Nano-imprint lithography tools
- Step and flash imprint lithography (S-FIL) tools

f.3. Equipment "specially designed" for mask making having all of the following:

f.3.a. A deflected focused electron beam, ion beam or "laser" beam; and

f.3.b. Having any of the following:

f.3.b.1. A Full-Width Half-Maximum (FWHM) spot size smaller than 65 nm and an image placement less than 17 nm (mean + 3 sigma); or

f.3.b.2. [Reserved]

f.3.b.3. A second-layer overlay error of less than 23 nm (mean + 3 sigma) on the mask;

f.4. Equipment designed for device processing using direct writing methods, having all of the following:

f.4.a. A deflected focused electron beam; and

f.4.b. Having any of the following:

f.4.b.1. A minimum beam size equal to or smaller than 15 nm; or

f.4.b.2. An overlay error less than 27 nm (mean + 3 sigma);

g. Masks and reticles, designed for integrated circuits controlled by 3A001;

h. Multi-layer masks with a phase shift layer not specified by 3B001.g and designed to be used by lithography equipment having a light source wavelength less than 245 nm;

Note: 3B001.h. does not control multi-layer masks with a phase shift layer designed for the fabrication of memory devices not controlled by 3A001.

N.B.: For masks and reticles, "specially designed" for optical sensors, see 6B002.

i. Imprint lithography templates designed for integrated circuits by 3A001;

j. Mask "substrate blanks" with multilayer reflector structure consisting of molybdenum and silicon, and having all of the following:

j.1. "Specially designed" for "Extreme Ultraviolet" ("EUV") lithography; and

j.2. Compliant with SEMI Standard P37;

k. Equipment designed for ion beam deposition or physical vapor deposition of a multi-layer reflector for "EUV" masks;

l. "EUV" pellicles;

m. Equipment for manufacturing "EUV" pellicles;

n. Equipment designed for coating, depositing, baking, or developing photoresist formulated for "EUV" lithography;

o. Annealing equipment, operating in a vacuum (equal to or less than 0.01 Pa) environment, performing any of the following:

o.1. Reflow of copper (Cu) to minimize or eliminate voids or seams in copper (Cu) metal interconnects; or

o.2. Reflow of cobalt (Co) or tungsten (W) fill metal to minimize or eliminate voids or seams;

p. Removal and cleaning equipment as follows:

p.1. Equipment designed for removing polymeric residue and copper oxide (CuO) film and enabling deposition of copper (Cu) metal in a vacuum (equal to or less than 0.01 Pa) environment;

p.2. Single wafer wet cleaning equipment with surface modification drying; or

p.3. Equipment designed for dry surface oxide removal preclean or dry surface decontamination.

Note to 3B001.p.1 and p.3: These controls do not apply to deposition equipment.

* * * * *

3B991 Equipment not controlled by 3B001, for the manufacture of electronic "parts," "components," and materials, and "specially designed" "parts," "components," and "accessories" therefor.

License Requirements

Reason for Control: AT

Control(s)	Country chart (see Supp. No. 1 to part 738)
------------	---

AT applies to entire entry.	AT Column 1.
-----------------------------	--------------

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

LVS: N/A

GBS: N/A

List of Items Controlled

Related Controls: N/A

Related Definitions: 'Sputtering' is an overlay coating process wherein positively charged ions are accelerated by an electric field towards the surface of a target (coating material). The kinetic energy of the impacting ions is sufficient to cause target surface atoms to be released and deposited on the substrate. (**Note:** Triode, magnetron or radio frequency sputtering to increase adhesion of coating and rate of deposition are ordinary modifications of the process.)

Items:

a. Equipment "specially designed" for the manufacture of electron tubes, optical elements and "specially designed" "parts" and "components" therefor controlled by 3A001 or 3A991;

b. Equipment "specially designed" for the manufacture of semiconductor devices, integrated circuits and "electronic assemblies", as follows, and systems incorporating or having the characteristics of such equipment:

Note: 3B991.b also controls equipment used or modified for use in the manufacture of other devices, such as imaging devices, electro-optical devices, acoustic-wave devices.

b.1. Equipment for the processing of materials for the manufacture of devices, "parts" and "components" as specified in the heading of 3B991.b, as follows:

Note: 3B991 does not control quartz furnace tubes, furnace liners, paddles, boats (except "specially designed" caged boats), bubblers, cassettes or crucibles "specially designed" for the processing equipment controlled by 3B991.b.1.

b.1.a. Equipment for producing polycrystalline silicon and materials controlled by 3C001;

b.1.b. Equipment "specially designed" for purifying or processing III/V and II/VI semiconductor materials controlled by 3C001, 3C002, 3C003, 3C004, or 3C005 except crystal pullers, for which see 3B991.b.1.c below;

b.1.c. Crystal pullers and furnaces, as follows:

Note: 3B991.b.1.c does not control diffusion and oxidation furnaces.

b.1.c.1. Annealing or recrystallizing equipment other than constant temperature furnaces employing high rates of energy transfer capable of processing wafers at a rate exceeding 0.005 m² per minute;

b.1.c.2. "Stored program controlled" crystal pullers having any of the following characteristics:

b.1.c.2.a. Rechargeable without replacing the crucible container;

b.1.c.2.b. Capable of operation at pressures above 2.5 x 10⁵ Pa; or

b.1.c.2.c. Capable of pulling crystals of a diameter exceeding 100 mm;

b.1.d. "Stored program controlled" equipment for epitaxial growth having any of the following characteristics:

b.1.d.1. Capable of producing silicon layer with a thickness uniform to less than ± 2.5% across a distance of 200 mm or more;

b.1.d.2. Capable of producing a layer of any material other than silicon with a thickness

uniformity across the wafer of equal to or better than $\pm 3.5\%$; or

b.1.d.3. Rotation of individual wafers during processing;

b.1.e. Molecular beam epitaxial growth equipment;

b.1.f. Magnetically enhanced 'sputtering' equipment with "specially designed" integral load locks capable of transferring wafers in an isolated vacuum environment;

b.1.g. Equipment "specially designed" for ion implantation, ion-enhanced or photo-enhanced diffusion, having any of the following characteristics:

b.1.g.1. Patterning capability;

b.1.g.2. Beam energy (accelerating voltage) exceeding 200 keV;

b.1.g.3. Optimized to operate at a beam energy (accelerating voltage) of less than 10 keV; or

b.1.g.4. Capable of high energy oxygen implant into a heated "substrate";

b.1.h. "Stored program controlled" equipment for the selective removal (etching) by means of anisotropic dry methods (e.g., plasma), as follows:

b.1.h.1. Batch types having either of the following:

b.1.h.1.a. End-point detection, other than optical emission spectroscopy types; or

b.1.h.1.b. Reactor operational (etching) pressure of 26.66 Pa or less;

b.1.h.2. Single wafer types having any of the following:

b.1.h.2.a. End-point detection, other than optical emission spectroscopy types;

b.1.h.2.b. Reactor operational (etching) pressure of 26.66 Pa or less; or

b.1.h.2.c. Cassette-to-cassette and load locks wafer handling;

Notes: 1. "Batch types" refers to machines not "specially designed" for production processing of single wafers. Such machines can process two or more wafers simultaneously with common process parameters, e.g., RF power, temperature, etch gas species, flow rates.

2. "Single wafer types" refers to machines "specially designed" for production processing of single wafers. These machines may use automatic wafer handling techniques to load a single wafer into the equipment for processing. The definition includes equipment that can load and process several wafers but where the etching parameters, e.g., RF power or end point, can be independently determined for each individual wafer.

b.1.i. "Chemical vapor deposition" (CVD) equipment, e.g., plasma-enhanced CVD (PECVD) or photo-enhanced CVD, for semiconductor device manufacturing, having either of the following capabilities, for deposition of oxides, nitrides, metals or polysilicon:

b.1.i.1. "Chemical vapor deposition" equipment operating below 10^5 Pa; or

b.1.i.2. PECVD equipment operating either below 60 Pa (450 millitorr) or having automatic cassette-to-cassette and load lock wafer handling;

Note: 3B991.b.1.i does not control low pressure "chemical vapor deposition" (LPCVD) systems or reactive "sputtering" equipment.

b.1.j. Electron beam systems "specially designed" or modified for mask making or

semiconductor device processing having any of the following characteristics:

b.1.j.1. Electrostatic beam deflection;

b.1.j.2. Shaped, non-Gaussian beam profile;

b.1.j.3. Digital-to-analog conversion rate exceeding 3 MHz;

b.1.j.4. Digital-to-analog conversion accuracy exceeding 12 bit; or

b.1.j.5. Target-to-beam position feedback control precision of 1 micrometer or finer;

Note: 3B991.b.1.j does not control electron beam deposition systems or general purpose scanning electron microscopes.

b.1.k. Surface finishing equipment for the processing of semiconductor wafers as follows:

b.1.k.1. "Specially designed" equipment for backside processing of wafers thinner than 100 micrometer and the subsequent separation thereof; or

b.1.k.2. "Specially designed" equipment for achieving a surface roughness of the active surface of a processed wafer with a two-sigma value of 2 micrometer or less, total indicator reading (TIR);

Note: 3B991.b.1.k does not control single-side lapping and polishing equipment for wafer surface finishing.

b.1.l. Interconnection equipment which includes common single or multiple vacuum chambers "specially designed" to permit the integration of any equipment controlled by 3B991 into a complete system;

b.1.m. "Stored program controlled" equipment using "lasers" for the repair or trimming of "monolithic integrated circuits" with either of the following characteristics:

b.1.m.1. Positioning accuracy less than ± 1 micrometer; or

b.1.m.2. Spot size (kerf width) less than 3 micrometer.

b.2. Masks, mask "substrates," mask-making equipment and image transfer equipment for the manufacture of devices, "parts" and "components" as specified in the heading of 3B991, as follows:

Note: The term "masks" refers to those used in electron beam lithography, X-ray lithography, and ultraviolet lithography, as well as the usual ultraviolet and visible photo-lithography.

b.2.a. Finished masks, reticles and designs thereof, except:

b.2.a.1. Finished masks or reticles for the production of unembargoed integrated circuits; or

b.2.a.2. Masks or reticles, having both of the following characteristics:

b.2.a.2.a. Their design is based on geometries of 2.5 micrometer or more; and

b.2.a.2.b. The design does not include special features to alter the intended use by means of production equipment or "software";

b.2.b. Mask "substrates" as follows:

b.2.b.1. Hard surface (e.g., chromium, silicon, molybdenum) coated "substrates" (e.g., glass, quartz, sapphire) for the preparation of masks having dimensions exceeding $125 \text{ mm} \times 125 \text{ mm}$; or

b.2.b.2. "Substrates" "specially designed" for X-ray masks;

b.2.c. Equipment, other than general purpose computers, "specially designed" for computer aided design (CAD) of semiconductor devices or integrated circuits;

b.2.d. Equipment or machines, as follows, for mask or reticle fabrication:

b.2.d.1. Photo-optical step and repeat cameras capable of producing arrays larger than $100 \text{ mm} \times 100 \text{ mm}$, or capable of producing a single exposure larger than $6 \text{ mm} \times 6 \text{ mm}$ in the image (i.e., focal) plane, or capable of producing line widths of less than 2.5 micrometer in the photoresist on the "substrate";

b.2.d.2. Mask or reticle fabrication equipment using ion or "laser" beam lithography capable of producing line widths of less than 2.5 micrometer; or

b.2.d.3. Equipment or holders for altering masks or reticles or adding pellicles to remove defects;

Note: 3B991.b.2.d.1 and b.2.d.2 do not control mask fabrication equipment using photo-optical methods which was either commercially available before the 1st January, 1980, or has a performance no better than such equipment.

b.2.e. "Stored program controlled" equipment for the inspection of masks, reticles or pellicles with:

b.2.e.1. A resolution of 0.25 micrometer or finer; and

b.2.e.2. A precision of 0.75 micrometer or finer over a distance in one or two coordinates of 63.5 mm or more;

Note: 3B991.b.2.e does not control general purpose scanning electron microscopes except when "specially designed" and instrumented for automatic pattern inspection.

b.2.f. Align and expose equipment for wafer production using photo-optical or X-ray methods, e.g., lithography equipment, including both projection image transfer equipment and step and repeat (direct step on wafer) or step and scan (scanner) equipment, capable of performing any of the following functions:

Note: 3B991.b.2.f does not control photo-optical contact and proximity mask align and expose equipment or contact image transfer equipment.

b.2.f.1. Production of a pattern size of less than 2.5 micrometer;

b.2.f.2. Alignment with a precision finer than ± 0.25 micrometer (3 sigma);

b.2.f.3. Machine-to-machine overlay no better than ± 0.3 micrometer; or

b.2.f.4. A light source wavelength shorter than 400 nm;

b.2.g. Electron beam, ion beam or X-ray equipment for projection image transfer capable of producing patterns less than 2.5 micrometer;

Note: For focused, deflected-beam systems (direct write systems), see 3B991.b.1.j or b.10.

b.2.h. Equipment using "lasers" for direct write on wafers capable of producing patterns less than 2.5 micrometer.

b.3. Equipment for the assembly of integrated circuits, as follows:

b.3.a. "Stored program controlled" die bonders having all of the following characteristics:

b.3.a.1. "Specially designed" for "hybrid integrated circuits";

b.3.a.2. X-Y stage positioning travel exceeding $37.5 \times 37.5 \text{ mm}$; and

b.3.a.3. Placement accuracy in the X-Y plane of finer than ± 10 micrometer;

b.3.b. “Stored program controlled” equipment for producing multiple bonds in a single operation (e.g., beam lead bonders, chip carrier bonders, tape bonders);

b.3.c. Semi-automatic or automatic hot cap sealers, in which the cap is heated locally to a higher temperature than the body of the package, “specially designed” for ceramic microcircuit packages controlled by 3A001 and that have a throughput equal to or more than one package per minute.

Note: 3B991.b.3 does not control general purpose resistance type spot welders.

b.4. Filters for clean rooms capable of providing an air environment of 10 or less particles of 0.3 micrometer or smaller per 0.02832 m³ and filter materials therefor.

* * * * *

3D001 “Software” “specially designed” for the “development” or “production” of commodities controlled by 3A001.b to 3A002.h, 3A090, or 3B (except 3B991 and 3B992).

License Requirements

Reason for Control: NS, RS, AT

<i>Control(s)</i>	<i>Country chart (see Supp. No. 1 to part 738)</i>
NS applies to “software” for commodities controlled by 3A001.b to 3A001.h, 3A001.z, and 3B (except 3B001.a.4, c, d, f.1.b, j to p, 3B002.b and c).	NS Column 1.
NS applies to “software” for commodities controlled by 3B001.a.4, c, d, f.1.b, j to p, 3B002.b and c.	To or within destinations specified in Country Group D:5 of supplement no. 1 to part 740 of the EAR or Macau. See § 742.4(a)(4) of the EAR.
RS applies to “software” for commodities controlled by 3A001.z and 3A090.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.
AT applies to entire entry.	AT Column 1.

Reporting Requirements

See § 743.1 of the EAR for reporting requirements for exports under License Exceptions, Special Comprehensive Licenses, and Validated End-User authorizations.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

TSR: Yes, except for “software” “specially designed” for the “development” or “production” of Traveling Wave Tube

Amplifiers described in 3A001.b.8 having operating frequencies exceeding 18 GHz; or commodities specified in 3A090, 3B001.a.4, c, d, f.1.b, j to p, and 3B002.b and c.

Note: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for ECCN 3D001 “software” for commodities controlled by 3A001.z and 3A090.

Special Conditions for STA

STA: License Exception STA may not be used to ship or transmit “software” “specially designed” for the “development” or “production” of equipment specified by 3A090, 3A002.g.1, 3B001.a.4, a.2, c, d, f.1.b, j to p, or 3B002.b and c to any of the destinations listed in Country Group A:6 (See Supplement No.1 to part 740 of the EAR).

List of Items Controlled

Related Controls: N/A
Related Definitions: N/A
Items:

The list of items controlled is contained in the ECCN heading.

3D002 “Software” “specially designed” for the “use” of equipment controlled by 3B001.a to .f and .j to .p, or 3B002.

License Requirements

Reason for Control: NS, RS, AT

<i>Control(s)</i>	<i>Country chart (see Supp. No. 1 to part 738)</i>
NS applies to entire entry, except “software” for 3B001.a.4 c, d, f.1.b, j to p, 3B002.b and c.	NS Column 1.
NS applies to “software” for 3B001.a.4, c, d, f.1.b.j to p, 3B002.b and c.	To or within Macau or a destination specified in Country Group D:5 of supplement no. 1 to part 740 of the EAR. See § 742.4(a)(4) of the EAR.
RS applies to “software” for 3B001.a.4, c, d, f.1.b, j to p, 3B002.b and c.	To or within Macau or a destination specified in Country Group D:5 of supplement no. 1 to part 740 of the EAR. See § 742.6(a)(6) of the EAR.
AT applies to entire entry.	AT Column 1.

License Requirements Note: See § 744.17 of the EAR for additional license requirements for microprocessors having a processing speed of 5 GFLOPS or more and an arithmetic logic unit with an access width of 32 bit or more, including those incorporating “information security” functionality, and associated “software” and “technology” for the “production” or “development” of such microprocessors.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

TSR: Yes, except N/A for RS.

List of Items Controlled

Related Controls: Also see 3D991.
Related Definitions: N/A
Items:

The list of items controlled is contained in the ECCN heading.

* * * * *

3E001 “Technology” according to the General Technology Note for the “development” or “production” of commodities controlled by 3A (except 3A980, 3A981, 3A991, 3A992, or 3A999), 3B (except 3B991 or 3B992) or 3C (except 3C992).

License Requirements

Reason for Control: NS, MT, NP, RS, AT

<i>Control(s)</i>	<i>Country chart (see Supp. No. 1 to part 738)</i>
NS applies to “technology” for commodities controlled by 3A001, 3A002, 3A003, 3B001 (except 3B001 a.4, c, d, f.1.b, j to p), 3B002 (except 3B002.b and c), or 3C001 to 3C006.	NS Column 1.
NS applies to “technology” for 3B001 a.4, c, d, f.1.b, j to p, 3B002.b and c.	To or within Macau or a destination specified in Country Group D:5 of supplement no. 1 to part 740 of the EAR. See § 742.4(a)(4) of the EAR.
MT applies to “technology” for commodities controlled by 3A001 or 3A101 for MT Reasons.	MT Column 1.
NP applies to “technology” for commodities controlled by 3A001, 3A201, or 3A225 to 3A234 for NP reasons.	NP Column 1.
RS applies to “technology” for commodities controlled in 3A090, when exported from Macau or a destination specified in Country Group D:5.	Worldwide (See § 742.6(a)(6)(ii).

Control(s) Country chart (see Supp. No. 1 to part 738)

RS applies to "technology" for commodities controlled by 3A001.z, 3A090. To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.

RS applies to "technology" for commodities controlled by 3B001.a.4, c, d, f.1.b, j to p, 3B002.b and c. To or within destinations specified in Country Group D:5 of supplement no. 1 to part 740 of the EAR or Macau. See § 742.6(a)(6)(i) of the EAR.

AT applies to entire entry. AT Column 1.

License Requirements Note: See § 744.17 of the EAR for additional license requirements for microprocessors having a processing speed of 5 GFLOPS or more and an arithmetic logic unit with an access width of 32 bit or more, including those incorporating "information security" functionality, and associated "software" and "technology" for the "production" or "development" of such microprocessors.

Reporting Requirements

See § 743.1 of the EAR for reporting requirements for exports under License Exceptions, Special Comprehensive Licenses, and Validated End-User authorizations.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

TSR: Yes, except N/A for MT, and "technology" for the "development" or "production" of: (a) vacuum electronic device amplifiers described in 3A001.b.8, having operating frequencies exceeding 19 GHz; (b) solar cells, coverglass-interconnect-cells or covered-interconnect-cells (CIC) "assemblies", solar arrays and/or solar panels described in 3A001.e.4; (c) "Monolithic Microwave Integrated Circuit" ("MMIC") amplifiers in 3A001.b.2; (d) discrete microwave transistors in 3A001.b.3; and (e) commodities described in 3A090, 3B001.a.4, c, d, f.1.b, j to p, 3B002.b and c.

Note: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for ECCN 3E001 "technology" for commodities controlled by 3A001.z, 3A090.

Special Conditions for STA

STA: License Exception STA may not be used to ship or transmit "technology" according to the General Technology Note for the "development" or "production" of equipment specified by ECCNs 3A002.g.1 or 3B001.a.2 to any of the destinations listed in Country Group A:6 (See Supplement No.1 to part 740 of the EAR). License Exception STA may not be used to

ship or transmit "technology" according to the General Technology Note for the "development" or "production" of components specified by ECCN 3A001.b.2, b.3, commodities specified in 3A090, 3B001.a.4, c, d, f.1.b, j to p, or 3B002.b and c, to any of the destinations listed in Country Group A:5 or A:6 (See Supplement No.1 to part 740 of the EAR).

List of Items Controlled

Related Controls: (1) "Technology" according to the General Technology Note for the "development" or "production" of certain "space-qualified" atomic frequency standards described in Category XV(e)(9), MMICs described in Category XV(e)(14), and oscillators described in Category XV(e)(15) of the USML are "subject to the ITAR" (see 22 CFR parts 120 through 130). See also 3E101, 3E201 and 9E515. (2) "Technology" for "development" or "production" of "Microwave Monolithic Integrated Circuits" ("MMIC") amplifiers in 3A001.b.2 is controlled in this ECCN 3E001; 5E001.d refers only to that additional "technology" "required" for telecommunications.

Related Definition: N/A Items:

The list of items controlled is contained in the ECCN heading.

Note 1: 3E001 does not control "technology" for equipment or "components" controlled by 3A003.

Note 2: 3E001 does not control "technology" for integrated circuits controlled by 3A001.a.3 to a.14 or .z, having all of the following:

(a) Using "technology" at or above 0.130 µm; and

(b) Incorporating multi-layer structures with three or fewer metal layers.

Note 3: 3E001 does not apply to 'Process Design Kits' ('PDKs') unless they include libraries implementing functions or technologies for items specified by 3A001.

Technical Note: For the purposes of 3E001 Note 3, a 'Process Design Kit' ('PDK') is a software tool provided by a semiconductor manufacturer to ensure that the required design practices and rules are taken into account in order to successfully produce a specific integrated circuit design in a specific semiconductor process, in accordance with technological and manufacturing constraints (each semiconductor manufacturing process has its particular 'PDK').

* * * * *

4A003 "Digital computers", "electronic assemblies", and related equipment therefor, as follows (see List of Items Controlled) and "specially designed" "components" therefor.

License Requirements

Reason for Control: NS, RS, CC, AT

Control(s) Country chart (see Supp. No. 1 to part 738)

NS applies to 4A003.b, .c, and .z.1. NS Column 1.

NS applies to 4A003.g, and z.2. NS Column 2.

Control(s) Country chart (see Supp. No. 1 to part 738)

RS applies to 4A003.z. To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.

CC applies to "digital computers" for computerized finger-print equipment. CC Column 1.

AT applies to entire entry (refer to 4A994 for controls on "digital computers" with a APP >0.0128 but ≤70 WT). AT Column 1.

Note: For all destinations, except those countries in Country Group E:1 or E:2 of Supplement No. 1 to part 740 of the EAR, no license is required (NLR) for computers with an "Adjusted Peak Performance" ("APP") not exceeding 70 Weighted TeraFLOPS (WT) and for "electronic assemblies" described in 4A003.c that are not capable of exceeding an "Adjusted Peak Performance" ("APP") exceeding 70 Weighted TeraFLOPS (WT) in aggregation, except certain transfers as set forth in § 746.3 (Iraq).

Reporting Requirements

Special Post Shipment Verification reporting and recordkeeping requirements for exports of computers to destinations in Computer Tier 3 may be found in § 743.2 of the EAR.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

LVS: \$5000; N/A for 4A003.b, and .c. GBS: Yes, for 4A003.g and "specially designed" "parts" and "components" therefor, exported separately or as part of a system.

APP: Yes, for computers controlled by 4A003.b, and "electronic assemblies" controlled by 4A003.c, to the exclusion of other technical parameters. See § 740.7 of the EAR.

NAC/ACA: Yes, for 4A003.z.

Note 1 to List Based License Exceptions:

Related equipment specified under ECCN 4A003.g, z.2, or z.4 are eligible for License Exception GBS if all the following conditions are met:

- 1. The related equipment is exported, reexported, or transferred (in-country) as part of a computer system,
2. The computer system is either designated as NLR or eligible for License Exception APP, and
3. The related equipment is eligible for License Exception APP.

Note 2: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for ECCN 4A003.z.

List of Items Controlled

Related Controls: See also ECCNs 4A090, 4A994 and 4A980.

Related Definitions: N/A

Items:

Note 1: 4A003 includes the following:

- ‘Vector processors’ (as defined in Note 7 of the ‘Technical Note on ‘Adjusted Peak Performance’ (‘APP’)’);
- Array processors;
- Digital signal processors;
- Logic processors;
- Equipment designed for ‘image enhancement.’

Note 2: The control status of the ‘digital computers’ and related equipment described in 4A003 is determined by the control status of other equipment or systems provided:

- a. The ‘digital computers’ or related equipment are essential for the operation of the other equipment or systems;
- b. The ‘digital computers’ or related equipment are not a ‘principal element’ of the other equipment or systems; and

N.B. 1: The control status of ‘signal processing’ or ‘image enhancement’ equipment ‘specially designed’ for other equipment with functions limited to those required for the other equipment is determined by the control status of the other equipment even if it exceeds the ‘principal element’ criterion.

N.B. 2: For the control status of ‘digital computers’ or related equipment for telecommunications equipment, see Category 5, Part 1 (Telecommunications).

- c. The ‘technology’ for the ‘digital computers’ and related equipment is determined by 4E.

a. [Reserved]

b. ‘Digital computers’ having an ‘Adjusted Peak Performance’ (‘APP’) exceeding 70 Weighted TeraFLOPS (WT);

c. ‘Electronic assemblies’ ‘specially designed’ or modified to be capable of enhancing performance by aggregation of processors so that the ‘APP’ of the aggregation exceeds the limit in 4A003.b.;

Note 1: 4A003.c applies only to ‘electronic assemblies’ and programmable interconnections not exceeding the limit in 4A003.b when shipped as unintegrated ‘electronic assemblies.’

Note 2: 4A003.c does not control ‘electronic assemblies’ ‘specially designed’ for a product or family of products whose maximum configuration does not exceed the limit of 4A003.b.

d. to f. [Reserved]

N.B.: For ‘electronic assemblies,’ modules or equipment, performing analog-to-digital conversions, see 3A002.h.

g. Equipment ‘specially designed’ for aggregating the performance of ‘digital computers’ by providing external interconnections which allow communications at unidirectional data rates exceeding 2.0 Gbyte/s per link.

Note: 4A003.g does not control internal interconnection equipment (e.g., backplanes, buses) passive interconnection equipment,

‘network access controllers’ or ‘communication channel controllers’.

h. through y. [Reserved]

z. Commodities specified in this ECCN 4A003 that also meet or exceed the performance parameters in 4A090.

z.1. Commodities specified in 4A003.b or .c that also meet or exceed the performance parameters in ECCN 4A090; or

z.2. Commodities specified in 4A003.g that also meet or exceed the performance parameters in ECCN 4A090.

4A004 Computers as follows (see List of Items Controlled) and ‘specially designed’ related equipment, ‘electronic assemblies’ and ‘components’ therefor.

License Requirements

Reason for Control: NS, RS, AT

Control(s)	Country chart (see Supp. No. 1 to part 738)
NS applies to entire entry.	NS Column 2.
RS applies to 4A004.z.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.
AT applies to entire entry.	AT Column 1.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

LVS: \$5000

GBS: N/A

NAC/ACA: Yes, for 4A004.z.

Note: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for ECCN 4A004.z.

List of Items Controlled

Related Controls: See also ECCN 4A090.

Related Definitions: N/A

Items:

- a. ‘Systolic array computers’;
- b. ‘Neural computers’;
- c. ‘Optical computers’.

Technical Notes:

1. For the purposes of 4A004.a, ‘systolic array computers’ are computers where the flow and modification of the data is dynamically controllable at the logic gate level by the user.

2. For the purposes of 4A004.b, ‘neural computers’ are computational devices designed or modified to mimic the behaviour of a neuron or a collection of neurons, i.e., computational devices which are distinguished by their hardware capability to modulate the weights and numbers of the interconnections of a multiplicity of computational components based on previous data.

3. For the purposes of 4A004.c, ‘optical computers’ are computers designed or

modified to use light to represent data and whose computational logic elements are based on directly coupled optical devices.

d. through y. [Reserved]

z. Commodities that are described in 4A004 and that also meet or exceed the performance parameters in 4A090.

4A005 ‘Systems,’ ‘equipment,’ and ‘components’ therefor, ‘specially designed’ or modified for the generation, command and control, or delivery of ‘intrusion software’ (see List of Items Controlled).

License Requirements

Reason for Control: NS, RS, AT

Control(s)	Country chart (see Supp. No. 1 to part 738)
NS applies to entire entry.	NS Column 1.
RS applies to items controlled by 4A005.z.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.
AT applies to entire entry.	AT Column 1.

Reporting Requirements

See § 743.1 of the EAR for reporting requirements for exports under License Exceptions, and Validated End-User authorizations.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

LVS: N/A

GBS: N/A

APP: N/A

ACE: Yes, except to Country Group E:1 or E:2. See § 740.22 of the EAR for eligibility criteria.

NAC/ACA: Yes, for 4A005.z.

Note: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for ECCN 4A005.z.

Special Conditions for STA

STA: License Exception STA may not be used to ship items specified by ECCN 4A005.

List of Items Controlled

Related Controls: (1) Defense articles described in USML Category XI(b), and software directly related to a defense article, are ‘subject to the ITAR’ (see 22 CFR parts 120 through 130). (2) See also ECCN 4A090.

Related Definitions: N/A

Items:

The list of items controlled is contained in the ECCN heading, except for the commodities controlled under 4A005.z.
a. through y. [Reserved]

z. Commodities that are specified in 4A005 that also meet or exceed the performance parameters in 4A090.

4A090 Computers as follows (see List of Items Controlled) and related equipment, "electronic assemblies," and "components" therefor.

License Requirements

Reason for Control: RS, AT

<i>Control(s)</i>	<i>Country chart (see Supp. No. 1 to part 738)</i>
RS applies to entire entry.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.
AT applies to entire entry.	AT Column 1.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

LVS: N/A

GBS: N/A

NAC/ACA: Yes, for 4A090, if the item incorporates a 3A090.a IC that is not designed or marketed for use in datacenters and has a 'total processing performance' of 4800 or more, or if the ECCN 4A090 item incorporates a 3A090.b IC, if the item is designed or marketed for use in datacenters.

List of Items Controlled

Related Controls: (1) For associated "software" for commodities in this ECCN, see 4D090, 5D002.z, and 5D992.z and for associated "technology" for commodities in this ECCN, see 4E001. (2) Also ECCNs 4A003.z, 4A004.z, 4A005.z, 5A002.z, 5A004.z, and 5A992.z.

Related Definitions: N/A
Items:

a. Computers, "electronic assemblies," and "components" containing integrated circuits, any of which meets or exceeds the limits in 3A090.a.

b. Computers, "electronic assemblies," and "components" containing integrated circuits, any of which meets or exceeds the limits in 3A090.b.

Technical Note: For purposes of 4A090.a and .b, computers include "digital computers," "hybrid computers," and analog computers.

* * * * *

4D001 "Software" as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, RS, CC, AT

<i>Control(s)</i>	<i>Country chart (see Supp. No. 1 to part 738)</i>
NS applies to entire entry.	NS Column 1.
RS applies to "software" for commodities controlled by 4A003.z, 4A004.z, and 4A005.z.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.
CC applies to "software" for computerized finger-print equipment controlled by 4A003 for CC reasons.	CC Column 1.
AT applies to entire entry.	AT Column 1.

Reporting Requirements

See § 743.1 of the EAR for reporting requirements for exports under License Exceptions, and Validated End-User authorizations.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

TSR: Yes, except for "software" for the "development" or "production" of the following:

- (1) Commodities with an "Adjusted Peak Performance" ("APP") exceeding 29 WT; or
- (2) Commodities controlled by 4A005 or "software" controlled by 4D004.

APP: Yes to specific countries (see § 740.7 of the EAR for eligibility criteria).

ACE: Yes for 4D001.a (for the "development", "production" or "use" of equipment or "software" specified in ECCN 4A005 or 4D004), except to Country Group E:1 or E:2. See § 740.22 of the EAR for eligibility criteria.

Note: See § 740.2(a)(9)(ii) for license exception restrictions for "software" for commodities controlled by 4A003.z, 4A004.z, and 4A005.z.

Special Conditions for STA

STA: License Exception STA may not be used to ship or transmit "software" "specially designed" or modified for the "development" or "production" of equipment specified by ECCN 4A001.a.2 or for the "development" or "production" of "digital computers" having an 'Adjusted Peak Performance' ('APP') exceeding 29 Weighted TeraFLOPS (WT) to any of the destinations listed in Country Group A:6 (See Supplement No.1 to part 740 of the EAR); and may not be used to ship or transmit "software" specified in 4D001.a "specially designed" for the "development" or "production" of equipment specified by ECCN 4A005 to any of the destinations listed in Country Group A:5 or A:6.

List of Items Controlled

Related Controls: N/A

Related Definitions: N/A
Items:

a. "Software" "specially designed" or modified for the "development" or "production", of equipment or "software" controlled by 4A001, 4A003, 4A004, 4A005 or 4D (except 4D090, 4D980, 4D993 or 4D994).

b. "Software", other than that controlled by 4D001.a, "specially designed" or modified for the "development" or "production" of equipment as follows:

b.1. "Digital computers" having an "Adjusted Peak Performance" ("APP") exceeding 24 Weighted TeraFLOPS (WT);

b.2. "Electronic assemblies" "specially designed" or modified for enhancing performance by aggregation of processors so that the "APP" of the aggregation exceeds the limit in 4D001.b.1.

* * * * *

4E001 "Technology" as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, MT, RS, CC, AT

<i>Control(s)</i>	<i>Country chart (See Supp. No. 1 to part 738)</i>
NS applies to entire entry, except for technology for 4A090 or "software" specified by 4D090.	NS Column 1.
MT applies to "technology" for items controlled by 4A001.a and 4A101 for MT reasons.	MT Column 1.
RS applies to "technology" for commodities controlled by 4A003.z, 4A004.z, 4A005.z, 4A090 or "software" specified by 4D001 (for 4A003.z, 4A004.z, and 4A005.z), 4D090.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.
CC applies to "technology" for computerized finger-print equipment controlled by 4A003 for CC reasons.	CC Column 1.
AT applies to entire entry.	AT Column 1.

Reporting Requirements

See § 743.1 of the EAR for reporting requirements for exports under License Exceptions, and Validated End-User authorizations.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

TSR: Yes, except for the following:

(1) “Technology” for the “development” or “production” of commodities with an “Adjusted Peak Performance” (“APP”) exceeding 70 WT or for the “development” or “production” of commodities controlled by 4A005 or “software” controlled by 4D004; or

(2) “Technology” for the “development” of “intrusion software”.

APP: Yes to specific countries (see § 740.7 of the EAR for eligibility criteria).

ACE: Yes for 4E001.a (for the “development”, “production” or “use” of equipment or “software” specified in ECCN 4A005 or 4D004) and for 4E001.c, except to Country Group E:1 or E:2. See § 740.22 of the EAR for eligibility criteria.

Note: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for technology for .z paragraphs under ECCNs 4A003, 4A004, or 4A005 or “software” specified by 4D001 (for 4A003.z, 4A004.z, and 4A005.z).

Special Conditions for STA

STA: License Exception STA may not be used to ship or transmit “technology” according to the General Technology Note for the “development” or “production” of any of the following equipment or “software”: a. Equipment specified by ECCN 4A001.a.2; b. “Digital computers” having an ‘Adjusted Peak Performance’ (‘APP’) exceeding 70 Weighted TeraFLOPS (WT); or c. “software” specified in the License Exception STA paragraph found in the License Exception section of ECCN 4D001 to any of the destinations listed in Country Group A:6 (See Supplement No. 1 to part 740 of the EAR); and may not be used to ship or transmit “technology” specified in 4E001.a (for the “development”, “production” or “use” of equipment or “software” specified in ECCN 4A005, 4A090, or “software” specified by 4D004 or 4D090); and 4E001.c to any of the destinations listed in Country Group A:5 or A:6.

List of Items Controlled

Related Controls: N/A
 Related Definitions: N/A
 Items:

a. “Technology” according to the General Technology Note, for the “development”, “production”, or “use” of equipment or “software” controlled by 4A (except 4A980 or 4A994 and “use” of equipment controlled under 4A090) or 4D (except 4D980, 4D993, 4D994 and “use” of software controlled under 4D090).

b. “Technology” according to the General Technology Note, other than that controlled by 4E001.a, for the “development” or “production” of equipment as follows:

b.1. “Digital computers” having an “Adjusted Peak Performance” (“APP”) exceeding 24 Weighted TeraFLOPS (WT);

b.2. “Electronic assemblies” “specially designed” or modified for enhancing performance by aggregation of processors so that the “APP” of the aggregation exceeds the limit in 4E001.b.1.

c. “Technology” for the “development” of “intrusion software.”

Note 1: 4E001.a and 4E001.c do not apply to “vulnerability disclosure” or “cyber incident response”.

Note 2: Note 1 does not diminish national authorities’ rights to ascertain compliance with 4E001.a and 4E001.c.

* * * * *

Category 5—Telecommunications and “Information Security”

* * * * *

Category 5—Telecommunications and “Information Security”

* * * * *

5A002 “Information security” systems, equipment and “components,” as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, RS, AT, EI

Control(s)	Country chart (See Supp. No. 1 to part 738)
------------	---

NS applies to entire entry.	NS Column 1.
RS applies to items controlled by 5A002.z.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.
AT applies to entire entry.	AT Column 1.
EI applies to entire entry.	Refer to § 742.15 of the EAR.

License Requirements Note: See § 744.17 of the EAR for additional license requirements for microprocessors having a processing speed of 5 GFLOPS or more and an arithmetic logic unit with an access width of 32 bit or more, including those incorporating “information security” functionality, and associated “software” and “technology” for the “production” or “development” of such microprocessors.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

LVS: Yes: \$500 for “components,” N/A for systems and equipment.

GBS: N/A

ENC: Yes for certain EI controlled commodities, see § 740.17 of the EAR for eligibility.

NAC/ACA: Yes, for 5A002.z.

Note: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for ECCN 5A002.z.

List of Items Controlled

Related Controls: (1) ECCN 5A002.a controls “components” providing the means or functions necessary for “information security.” All such “components” are presumptively “specially designed” and controlled by 5A002.a. (2) See USML

Categories XI (including XI(b)) and XIII(b) (including XIII(b)(2)) for controls on systems, equipment, and components described in 5A002.d or .e that are “subject to the ITAR” (see 22 CFR parts 120 through 130). (3) For “satellite navigation system” receiving equipment containing or employing decryption see 7A005, and for related decryption “software” and “technology” see 7D005 and 7E001. (4) Noting that items may be controlled elsewhere on the CCL, examples of items not controlled by ECCN 5A002.a.4 include the following: (a) An automobile where the only ‘cryptography for data confidentiality’ having a ‘described security algorithm’ is performed by a Category 5—Part 2 Note 3 eligible mobile telephone that is built into the car. In this case, secure phone communications support a non-primary function of the automobile but the mobile telephone (equipment), as a standalone item, is not controlled by ECCN 5A002 because it is excluded by the Cryptography Note (Note 3) (See ECCN 5A992.c). (b) An exercise bike with an embedded Category 5—Part 2 Note 3 eligible web browser, where the only controlled cryptography is performed by the web browser. In this case, secure web browsing supports a non-primary function of the exercise bike but the web browser (“software”), as a standalone item, is not controlled by ECCN 5D002 because it is excluded by the Cryptography Note (Note 3) (See ECCN 5D992.c). (5) After classification or self-classification in accordance with § 740.17(b) of the EAR, mass market encryption commodities that meet eligibility requirements are released from “EI” and “NS” controls. These commodities are designated 5A992.c. (6) See also ECCNs 3A090 and 4A090.

Related Definitions: N/A

Items:

a. Designed or modified to use ‘cryptography for data confidentiality’ having a ‘described security algorithm’, where that cryptographic capability is usable, has been activated, or can be activated by any means other than secure “cryptographic activation”, as follows:

a.1. Items having “information security” as a primary function;
 a.2. Digital communication or networking systems, equipment or components, not specified in paragraph 5A002.a.1;
 a.3. Computers, other items having information storage or processing as a primary function, and components therefor, not specified in paragraphs 5A002.a.1 or .a.2;
N.B.: For operating systems see also 5D002.a.1 and .c.1.

a.4. Items, not specified in paragraphs 5A002.a.1 to a.3, where the ‘cryptography for data confidentiality’ having a ‘described security algorithm’ meets all of the following:

a.4.a. It supports a non-primary function of the item; and

a.4.b. It is performed by incorporated equipment or “software” that would, as a standalone item, be specified by ECCNs 5A002, 5A003, 5A004, 5B002 or 5D002.

N.B. to paragraph a.4: See Related Control Paragraph (4) of this ECCN 5A002 for examples of items not controlled by 5A002.a.4.

Technical Notes:

1. For the purposes of 5A002.a, ‘cryptography for data confidentiality’ means “cryptography” that employs digital techniques and performs any cryptographic function other than any of the following:

1.a. “Authentication;”

1.b. Digital signature;

1.c. Data integrity;

1.d. Non-repudiation;

1.e. Digital rights management, including the execution of copy-protected “software;”

1.f. Encryption or decryption in support of entertainment, mass commercial broadcasts or medical records management; or

1.g. Key management in support of any function described in paragraphs 1.a to 1.f of this Technical Note paragraph 1.

2. For the purposes of 5A002.a, ‘described security algorithm’ means any of the following:

2.a. A “symmetric algorithm” employing a key length in excess of 56 bits, not including parity bits;

2.b. An “asymmetric algorithm” where the security of the algorithm is based on any of the following:

2.b.1. Factorization of integers in excess of 512 bits (e.g., RSA);

2.b.2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or

2.b.3. Discrete logarithms in a group other than mentioned in paragraph 2.b.2 of this Technical Note in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve); or

2.c. An “asymmetric algorithm” where the security of the algorithm is based on any of the following:

2.c.1. Shortest vector or closest vector problems associated with lattices (e.g., NewHope, Frodo, NTRUEncrypt, Kyber, Titanium);

2.c.2. Finding isogenies between Supersingular elliptic curves (e.g., Supersingular Isogeny Key Encapsulation); or

2.c.3. Decoding random codes (e.g., McEliece, Niederreiter).

Technical Note: An algorithm described by Technical Note 2.c. may be referred to as being post-quantum, quantum-safe or quantum-resistant.

Note 1: Details of items must be accessible and provided upon request, in order to establish any of the following:

a. Whether the item meets the criteria of 5A002.a.1 to a.4; or

b. Whether the cryptographic capability for data confidentiality specified by 5A002.a is usable without “cryptographic activation.”

Note 2: 5A002.a does not control any of the following items, or specially designed “information security” components therefor:

a. Smart cards and smart card ‘readers/writers’ as follows:

a.1. A smart card or an electronically readable personal document (e.g., token coin, e-passport) that meets any of the following:

a.1.a. The cryptographic capability meets all of the following:

a.1.a.1. It is restricted for use in any of the following:

a.1.a.1.a. Equipment or systems, not described by 5A002.a.1 to a.4;

a.1.a.1.b. Equipment or systems, not using ‘cryptography for data confidentiality’ having a ‘described security algorithm’; or

a.1.a.1.c. Equipment or systems, excluded from 5A002.a by entries b. to f. of this Note; and

a.1.a.2. It cannot be reprogrammed for any other use; or

a.1.b. Having all of the following:

a.1.b.1. It is specially designed and limited to allow protection of ‘personal data’ stored within;

a.1.b.2. Has been, or can only be, personalized for public or commercial transactions or individual identification; and

a.1.b.3. Where the cryptographic capability is not user-accessible;

Technical Note to paragraph a.1.b.1 of Note 2: For the purposes of 5A002.a Note 2.–a.1.b.1, ‘personal data’ includes any data specific to a particular person or entity, such as the amount of money stored and data necessary for “authentication.”

a.2. ‘Readers/writers’ specially designed or modified, and limited, for items specified by paragraph a.1 of this Note;

Technical Note to paragraph a.2 of Note 2: For the purposes of 5A002.a Note 2.a.2, ‘readers/writers’ include equipment that communicates with smart cards or electronically readable documents through a network.

b. Cryptographic equipment specially designed and limited for banking use or ‘money transactions’;

Technical Note to paragraph b. of Note 2: For the purposes of 5A002.a Note 2.b, ‘money transactions’ in 5A002 Note 2 paragraph b. includes the collection and settlement of fares or credit functions.

c. Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radio communication systems) that are not capable of transmitting encrypted data directly to another radiotelephone or equipment (other than Radio Access Network (RAN) equipment), nor of passing encrypted data through RAN equipment (e.g., Radio Network Controller (RNC) or Base Station Controller (BSC));

d. Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (i.e., a single, unrelayed hop between terminal and home base station) is less than 400 meters according to the manufacturer’s specifications;

e. Portable or mobile radiotelephones and similar client wireless devices for civil use, that implement only published or commercial cryptographic standards (except for anti-piracy functions, which may be non-published) and also meet the provisions of paragraphs a.2 to a.4 of the Cryptography Note (Note 3 in Category 5—Part 2), that have been customized for a specific civil industry application with features that do not affect the cryptographic functionality of these original non-customized devices;

f. Items, where the “information security” functionality is limited to wireless “personal area network” functionality implementing only published or commercial cryptographic standards;

g. Mobile telecommunications Radio Access Network (RAN) equipment designed

for civil use, which also meet the provisions of paragraphs a.2 to a.4 of the Cryptography Note (Note 3 in Category 5—Part 2), having an RF output power limited to 0.1W (20 dBm) or less, and supporting 16 or fewer concurrent users;

h. Routers, switches, gateways or relays, where the “information security” functionality is limited to the tasks of “Operations, Administration or Maintenance” (“OAM”) implementing only published or commercial cryptographic standards;

i. General purpose computing equipment or servers, where the “information security” functionality meets all of the following:

i.1. Uses only published or commercial cryptographic standards; and

i.2. Is any of the following:

i.2.a. Integral to a CPU that meets the provisions of Note 3 in Category 5—Part 2;

i.2.b. Integral to an operating system that is not specified by 5D002; or

i.2.c. Limited to “OAM” of the equipment; or

j. Items specially designed for a ‘connected civil industry application’, meeting all of the following:

j.1. Being any of the following:

j.1.a. A network-capable endpoint device meeting any of the following:

j.1.a.1. The “information security” functionality is limited to securing ‘non-arbitrary data’ or the tasks of “Operations, Administration or Maintenance” (“OAM”); or

j.1.a.2. The device is limited to a specific ‘connected civil industry application’; or

j.1.b. Networking equipment meeting all of the following:

j.1.b.1. Being specially designed to communicate with the devices specified by paragraph j.1.a. above; and

j.1.b.2. The “information security” functionality is limited to supporting the ‘connected civil industry application’ of devices specified by paragraph j.1.a. above, or the tasks of “OAM” of this networking equipment or of other items specified by paragraph j. of this Note; and

j.2. Where the “information security” functionality implements only published or commercial cryptographic standards, and the cryptographic functionality cannot easily be changed by the user.

Technical Notes:

1. For the purposes of 5A002.a Note 2.j, ‘connected civil industry application’ means a network-connected consumer or civil industry application other than “information security”, digital communication, general purpose networking or computing.

2. For the purposes of 5A002.a Note 2.j.1.a.1, ‘non-arbitrary data’ means sensor or metering data directly related to the stability, performance or physical measurement of a system (e.g., temperature, pressure, flow rate, mass, volume, voltage, physical location, etc.), that cannot be changed by the user of the device.

b. Being a ‘cryptographic activation token’;

Technical Note: For the purposes of 5A002.b, a ‘cryptographic activation token’ is an item designed or modified for any of the following:

1. For the purposes of 5A002.a Note 2.j, ‘connected civil industry application’ means a network-connected consumer or civil industry application other than “information security”, digital communication, general purpose networking or computing.

2. For the purposes of 5A002.a Note 2.j.1.a.1, ‘non-arbitrary data’ means sensor or metering data directly related to the stability, performance or physical measurement of a system (e.g., temperature, pressure, flow rate, mass, volume, voltage, physical location, etc.), that cannot be changed by the user of the device.

b. Being a ‘cryptographic activation token’;

Technical Note: For the purposes of 5A002.b, a ‘cryptographic activation token’ is an item designed or modified for any of the following:

1. For the purposes of 5A002.a Note 2.j, ‘connected civil industry application’ means a network-connected consumer or civil industry application other than “information security”, digital communication, general purpose networking or computing.

2. For the purposes of 5A002.a Note 2.j.1.a.1, ‘non-arbitrary data’ means sensor or metering data directly related to the stability, performance or physical measurement of a system (e.g., temperature, pressure, flow rate, mass, volume, voltage, physical location, etc.), that cannot be changed by the user of the device.

b. Being a ‘cryptographic activation token’;

Technical Note: For the purposes of 5A002.b, a ‘cryptographic activation token’ is an item designed or modified for any of the following:

1. For the purposes of 5A002.a Note 2.j, ‘connected civil industry application’ means a network-connected consumer or civil industry application other than “information security”, digital communication, general purpose networking or computing.

2. For the purposes of 5A002.a Note 2.j.1.a.1, ‘non-arbitrary data’ means sensor or metering data directly related to the stability, performance or physical measurement of a system (e.g., temperature, pressure, flow rate, mass, volume, voltage, physical location, etc.), that cannot be changed by the user of the device.

b. Being a ‘cryptographic activation token’;

Technical Note: For the purposes of 5A002.b, a ‘cryptographic activation token’ is an item designed or modified for any of the following:

1. For the purposes of 5A002.a Note 2.j, ‘connected civil industry application’ means a network-connected consumer or civil industry application other than “information security”, digital communication, general purpose networking or computing.

2. For the purposes of 5A002.a Note 2.j.1.a.1, ‘non-arbitrary data’ means sensor or metering data directly related to the stability, performance or physical measurement of a system (e.g., temperature, pressure, flow rate, mass, volume, voltage, physical location, etc.), that cannot be changed by the user of the device.

b. Being a ‘cryptographic activation token’;

Technical Note: For the purposes of 5A002.b, a ‘cryptographic activation token’ is an item designed or modified for any of the following:

1. For the purposes of 5A002.a Note 2.j, ‘connected civil industry application’ means a network-connected consumer or civil industry application other than “information security”, digital communication, general purpose networking or computing.

2. For the purposes of 5A002.a Note 2.j.1.a.1, ‘non-arbitrary data’ means sensor or metering data directly related to the stability, performance or physical measurement of a system (e.g., temperature, pressure, flow rate, mass, volume, voltage, physical location, etc.), that cannot be changed by the user of the device.

b. Being a ‘cryptographic activation token’;

Technical Note: For the purposes of 5A002.b, a ‘cryptographic activation token’ is an item designed or modified for any of the following:

1. For the purposes of 5A002.a Note 2.j, ‘connected civil industry application’ means a network-connected consumer or civil industry application other than “information security”, digital communication, general purpose networking or computing.

2. For the purposes of 5A002.a Note 2.j.1.a.1, ‘non-arbitrary data’ means sensor or metering data directly related to the stability, performance or physical measurement of a system (e.g., temperature, pressure, flow rate, mass, volume, voltage, physical location, etc.), that cannot be changed by the user of the device.

1. Converting, by means of “cryptographic activation”, an item not specified by Category 5-Part 2 into an item specified by 5A002.a or 5D002.c.1, and not released by the Cryptography Note (Note 3 in Category 5—Part 2); or

2. Enabling by means of “cryptographic activation”, additional functionality specified by 5A002.a of an item already specified by Category 5—Part 2;

c. Designed or modified to use or perform “quantum cryptography”;

Technical Note: For the purposes of 5A002.c, “quantum cryptography” is also known as Quantum Key Distribution (QKD).

d. Designed or modified to use cryptographic techniques to generate channelizing codes, scrambling codes or network identification codes, for systems using ultra-wideband modulation techniques and having any of the following:

d.1. A bandwidth exceeding 500 MHz; or
d.2. A “fractional bandwidth” of 20% or more;

e. Designed or modified to use cryptographic techniques to generate the spreading code for “spread spectrum” systems, not specified by 5A002.d, including the hopping code for “frequency hopping” systems.

f. through y. [Reserved]

z. Other commodities, as follows:

z.1. Commodities that are described in 5A002.a and that also meet or exceed the performance parameters in 3A090 or 4A090;

z.2. Commodities that are described in 5A002.b and that also meet or exceed the performance parameters in 3A090 or 4A090;

z.3. Commodities that are described in 5A002.c and that also meet or exceed the performance parameters in 3A090 or 4A090;

z.4. Commodities that are described in 5A002.d and that also meet or exceed the performance parameters in 3A090 or 4A090;

z.5. Commodities that are described in 5A002.e and that also meet or exceed the performance parameters in 3A090 or 4A090.

5A992 Equipment not controlled by 5A002 (see List of Items Controlled)

License Requirements

Reason for Control: RS, AT

<i>Control(s)</i>	<i>Country chart (see Supp. No. 1 to part 738)</i>
RS applies to items controlled by 5A992.z.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.
AT applies to entire entry.	AT Column 1.

License Requirements Note: See § 744.17 of the EAR for additional license requirements for microprocessors having a

processing speed of 5 GFLOPS or more and an arithmetic logic unit with an access width of 32 bit or more, including those incorporating “information security” functionality, and associated “software” and “technology” for the “production” or “development” of such microprocessors.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

LVS: N/A

GBS: N/A

NAC/ACA: Yes, for 5A992.z; N/A for all other 5A992 commodities.

Note: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for ECCN 5A992.z.

List of Items Controlled

Related Controls: See also ECCNs 3A090 and 4A090.

Related Definitions: N/A

Items:

- a. [Reserved]
- b. [Reserved]
- c. Commodities classified as mass market encryption commodities in accordance with § 740.17(b) of the EAR.
- d. through y. [Reserved]
- z. Commodities that are described in 5A992.c and that also meet or exceed the performance parameters in 3A090 or 4A090.

5A004 “Systems,” “equipment” and “components” for defeating, weakening or bypassing “information security,” as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, RS, AT, EI

<i>Control(s)</i>	<i>Country chart (see Supp. No. 1 to part 738)</i>
NS applies to entire entry.	NS Column 1.
RS applies to items controlled by 5A004.z.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.
AT applies to entire entry.	AT Column 1.
EI applies to entire entry.	Refer to § 742.15 of the EAR.

License Requirements: See § 744.17 of the EAR for additional license requirements for microprocessors having a processing speed of 5 GFLOPS or more and an arithmetic logic unit with an access width of 32 bit or more, including those incorporating “information security” functionality, and associated “software” and “technology” for the “production” or “development” of such microprocessors.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

LVS: Yes: \$500 for “components”.

N/A for systems and equipment.

GBS: N/A

ENC: Yes for certain EI controlled commodities. See § 740.17 of the EAR for eligibility.

NAC/ACA: Yes, for 5A004.z.

Note: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for ECCN 5A004.z.

List of Items Controlled

Related Controls: (1) ECCN 5A004.a controls “components” providing the means or functions necessary for “information security.” All such “components” are presumptively “specially designed” and controlled by 5A004.a. (2) See also ECCNs 3A090 and 4A090.

Related Definitions: N/A

Items:

- a. Designed or modified to perform ‘cryptanalytic functions.’
- Note:** 5A004.a includes systems or equipment, designed or modified to perform ‘cryptanalytic functions’ by means of reverse engineering.

Technical Note: For the purposes of 5A004.a, ‘cryptanalytic functions’ are functions designed to defeat cryptographic mechanisms in order to derive confidential variables or sensitive data, including clear text, passwords or cryptographic keys.

b. Items, not specified by ECCNs 4A005 or 5A004.a, designed to perform all of the following:

- b.1. ‘Extract raw data’ from a computing or communications device; and
- b.2. Circumvent “authentication” or authorisation controls of the device, in order to perform the function described in 5A004.b.1.

Technical Note: For the purposes of 5A004.b.1, ‘extract raw data’ from a computing or communications device means to retrieve binary data from a storage medium, e.g., RAM, flash or hard disk, of the device without interpretation by the device’s operating system or filesystem.

Note 1: 5A004.b does not apply to systems or equipment specially designed for the “development” or “production” of a computing or communications device.

Note 2: 5A004.b does not include:

- a. Debuggers, hypervisors;
- b. Items limited to logical data extraction;
- c. Data extraction items using chip-off or JTAG; or
- d. Items specially designed and limited to jail-breaking or rooting.

c. through y. [Reserved]

z. Other commodities, as follows:

z.1. Commodities that are described in 5A004.a and that also meet or exceed the performance parameters in 3A090 or 4A090;

z.2. Commodities that are described in 5A004.b and that also meet or exceed the performance parameters in 3A090 or 4A090.

* * * * *

5D002 “Software” as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, RS, AT, EI

<i>Control(s)</i>	<i>Country chart (see Supp. No. 1 to part 738)</i>
NS applies to entire entry.	NS Column 1.
RS applies to “software” controlled by 5D002.z.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.
AT applies to entire entry.	AT Column 1.
EI applies to “software” in 5D002.a.1, a.3, .b, c.1 and c.3, for commodities or “software” controlled for EI reasons in ECCN 5A002, 5A004 or 5D002.	Refer to § 742.15 of the EAR. Note: <i>Encryption software is controlled because of its functional capacity, and not because of any informational value of such software; such software is not accorded the same treatment under the EAR as other “software”; and for export licensing purposes, encryption software is treated under the EAR in the same manner as a commodity included in ECCN 5A002.</i>

License Requirements Note: See § 744.17 of the EAR for additional license requirements for microprocessors having a processing speed of 5 GFLOPS or more and an arithmetic logic unit with an access width of 32 bit or more, including those incorporating “information security” functionality, and associated “software” and “technology” for the “production” or “development” of such microprocessors.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

TSR: N/A

ENC: Yes for certain EI controlled software.

See § 740.17 of the EAR for eligibility.

NAC/ACA: Yes, for 5D002.z.

Note: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for ECCN 5D002.z.

List of Items Controlled

Related Controls: (1) After classification or self-classification in accordance with § 740.17(b) of the EAR, mass market encryption software that meets eligibility requirements is released from “EI” and “NS” controls. This software is designated as 5D992.c. (2) See also ECCNs 3D001 as it applies to “software” for commodities

controlled by 3A001.z and 3A090, and 4D001 as it applies to “software” for commodities controlled by 4A003.z, 4A004.z, and 4A005.z.

Related Definitions: 5D002.a controls “software” designed or modified to use “cryptography” employing digital or analog techniques to ensure “information security.”

Items:

- a. “Software” “specially designed” or modified for the “development,” “production” or “use” of any of the following:
 - a.1. Equipment specified by 5A002 or “software” specified by 5D002.c.1;
 - a.2. Equipment specified by 5A003 or “software” specified by 5D002.c.2; or
 - a.3. Equipment or “software”, as follows:
 - a.3.a. Equipment specified by 5A004.a or “software” specified by 5D002.c.3.a;
 - a.3.b. Equipment specified by 5A004.b or “software” specified by 5D002.c.3.b;
 - b. “Software” having the characteristics of a ‘cryptographic activation token’ specified by 5A002.b;
 - c. “Software” having the characteristics of, or performing or simulating the functions of, any of the following:
 - c.1. Equipment specified by 5A002.a, .c, .d or .e;
- Note:** *5D002.c.1 does not apply to “software” limited to the tasks of “OAM” implementing only published or commercial cryptographic standards.*
- c.2. Equipment specified by 5A003; or
 - c.3. Equipment, as follows:
 - c.3.a. Equipment specified by 5A004.a;
 - c.3.b. Equipment specified by 5A004.b.
- Note:** *5D002.c.3.b does not apply to “intrusion software”.*
- d. [Reserved]
- N.B.:** *See 5D002.b for items formerly specified in 5D002.d.*
- e. through y. [Reserved]

z. Other software, as follows:

- z.1. Software that is described in 5D002.a.1, and that also meet or exceed the performance parameters in 3D001 for 3A090 or 4D001 for 4A090;

- z.2. Software that is described in 5D002.a.2, and that also meet or exceed the performance parameters in 3D001 for 3A090 or 4D001 for 4A090;

- z.3. Software that is described in 5D002.a.3a, and that also meet or exceed the performance parameters in 3D001 for 3A090 or 4D001 for 4A090;

- z.4. Software that is described in 5D002.a.3.b, and that also meet or exceed the performance parameters in 3D001 for 3A090 or 4D001 for 4A090;

- z.5. Software that is described in 5D002.b and that also meet or exceed the performance parameters in 3D001 for 3A090 or 4D001 for 4A090;

- z.6. Software that is described in 5D002.c.1 and that also meet or exceed the performance parameters in 3D001 for 3A090 or 4D001 for 4A090;

- z.7. Software that is described in 5D002.c.2 and that also meet or exceed the performance parameters in 3D001 for 3A090 or 4D001 for 4A090;

- z.8. Software that is described in 5D002.c.3.a and that also meet or exceed the

performance parameters in 3D001 for 3A090 or 4D001 for 4A090; or

z.9. Software that is described in 5D002.c.3.b and that also meet or exceed the performance parameters in 3D001 for 3A090 or 4D001 for 4A090.

5D992 “Information Security” “software,” not controlled by 5D002, as follows (see List of Items Controlled).

License Requirements

Reason for Control: RS, AT

<i>Control(s)</i>	<i>Country chart (see Supp. No. 1 to part 738)</i>
RS applies to “software” controlled by 5D992.z.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.
AT applies to entire entry.	AT Column 1.

License Requirements Note: See § 744.17 of the EAR for additional license requirements for microprocessors having a processing speed of 5 GFLOPS or more and an arithmetic logic unit with an access width of 32 bit or more, including those incorporating “information security” functionality, and associated “software” and “technology” for the “production” or “development” of such microprocessors.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

TSR: N/A

NAC/ACA: Yes, for 5D992.z.

Note: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for ECCN 5D992.z.

List of Items Controlled

Related Controls: (1) This entry does not control “software” designed or modified to protect against malicious computer damage, e.g., viruses, where the use of “cryptography” is limited to authentication, digital signature and/or the decryption of data or files. (2) See also ECCNs 3D001 as it applies to “software” for commodities controlled by 3A001.z and 3A090, and 4D001 as it applies to “software” for commodities controlled by 4A003.z, 4A004.z, and 4A005.z.

Related Definitions: N/A

Items:

- a. [Reserved]
- b. [Reserved]
- c. “Software” classified as mass market encryption software in accordance with § 740.17(b) of the EAR.
- d. through y. [Reserved]
- z. Other software that is described in 5D992 and that also meet or exceed the performance parameters in 3D001 for 3A090 or 4D001 for 4A090.

5E002 “Technology” as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, RS, AT, EI

Control(s)	Country chart (see Supp. No. 1 to part 738)
NS applies to entire entry.	NS Column 1.
RS applies to “technology” for commodities controlled by 5A002.z or 5A004.z or “software” specified by 5D002 (for 5A002.z or 5A004.z commodities).	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.
AT applies to entire entry.	AT Column 1.
EI applies to “technology” in 5E002.a for commodities or “software” controlled for EI reasons in ECCNs 5A002, 5A004 or 5D002, and to “technology” in 5E002.b.	Refer to § 742.15 of the EAR.

License Requirements Notes:

(1) See § 744.17 of the EAR for additional license requirements for microprocessors having a processing speed of 5 GFLOPS or more and an arithmetic logic unit with an access width of 32 bit or more, including those incorporating “information security” functionality, and associated “software” and “technology” for the “production” or “development” of such microprocessors.

(2) When a person performs or provides technical assistance that incorporates, or otherwise draws upon, “technology” that was either obtained in the United States or is of U.S.-origin, then a release of the “technology” takes place. Such technical assistance, when rendered with the intent to aid in the “development” or “production” of encryption commodities or software that would be controlled for “EI” reasons under ECCN 5A002, 5A004 or 5D002, may require authorization under the EAR even if the underlying encryption algorithm to be implemented is from the public domain or is not of U.S.-origin.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

TSR: N/A

ENC: Yes for certain EI controlled technology. See § 740.17 of the EAR for eligibility.

Note: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for technology for .z paragraphs under ECCNs 5A002, 5A004 or “software” specified by 5D002 (for 5A002.z or 5A004.z commodities).

List of Items Controlled

Related Controls: See also 5E992. This entry does not control “technology” “required” for the “use” of equipment excluded from control under the Related Controls paragraph or the Technical Notes in ECCN 5A002 or “technology” related to equipment excluded from control under ECCN 5A002.

Related Definitions: N/A
Items:

a. “Technology” according to the General Technology Note for the “development,” “production” or “use” of equipment controlled by 5A002, 5A003, 5A004 or 5B002, or of “software” controlled by 5D002.a, z.1 through z.3, or 5D002.c, z.6 through z.8.

Note: 5E002.a does not apply to “technology” for items specified by 5A004.b, z.3 or z.4, 5D002.a.3.b, z.4, or 5D002.c.3.b.

b. “Technology” having the characteristics of a ‘cryptographic activation token’ specified by 5A002.b, z.2.

Note: 5E002 includes “information security” technical data resulting from procedures carried out to evaluate or determine the implementation of functions, features or techniques specified in Category 5—Part 2.

5E992 “Information Security” “technology” according to the General Technology Note, not controlled by 5E002, as follows (see List of Items Controlled).

License Requirements

Reason for Control: RS, AT

Control(s)	Country chart (see Supp. No. 1 to part 738)
RS applies to “technology” for commodities controlled by 5A992.z or “software” controlled by 5D992.z.	To or within destinations specified in Country Groups D:1, D:4, and D:5 of supplement no. 1 to part 740 of the EAR, excluding any destination also specified in Country Groups A:5 or A:6. See § 742.6(a)(6)(iii) of the EAR.
AT applies to entire entry.	AT Column 1.

License Requirements Note: See § 744.17 of the EAR for additional license requirements for microprocessors having a processing speed of 5 GFLOPS or more and an arithmetic logic unit with an access width of 32 bit or more, including those incorporating “information security” functionality, and associated “software” and “technology” for the “production” or “development” of such microprocessors.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

TSR: N/A

Note: See § 740.2(a)(9)(ii) of the EAR for license exception restrictions for technology for .z paragraphs under “technology” for commodities controlled by 5A992.z or “software” controlled by 5D992.z.

List of Items Controlled

Related Controls: N/A

Related Definitions: N/A

Items:

a. [Reserved]
b. “Technology”, n.e.s., for the “use” of mass market commodities controlled by 5A992 or mass market “software” controlled by 5D992.

* * * * *

■ 15. Supplement no. 6 to part 774 is amended by revising paragraphs (3)(iv) and (v) to read as follows:

Supplement No. 6 to Part 774— Sensitive List

* * * * *

(3) Category 3

* * * * *

(iv) 3D001—“Software” “specially designed” for the “development” or “production” of equipment controlled under 3A001.b.2, 3A001.b.3, equipment described under 3A001.b.2 or 3A001.b.3 that are controlled under 3A001.z, and 3A002.g.1.

(v) 3E001—“Technology” according to the General Technology Note for the “development” or “production” of equipment controlled under 3A001.b.2, 3A001.b.3, equipment described under 3A001.b.2 or 3A001.b.3 that are controlled under 3A001.z, and 3A002.g.1.

* * * * *

Thea D. Rozman Kendler,
Assistant Secretary for Export Administration.

[FR Doc. 2024-07004 Filed 3-29-24; 4:15 pm]

BILLING CODE 3510-33-P

Reader Aids

Federal Register

Vol. 89, No. 66

Thursday, April 4, 2024

CUSTOMER SERVICE AND INFORMATION

Federal Register/Code of Federal Regulations	
General Information, indexes and other finding aids	202-741-6000
Laws	741-6000
Presidential Documents	
Executive orders and proclamations	741-6000
The United States Government Manual	741-6000
Other Services	
Electronic and on-line services (voice)	741-6020
Privacy Act Compilation	741-6050

ELECTRONIC RESEARCH

World Wide Web

Full text of the daily Federal Register, CFR and other publications is located at: www.govinfo.gov.

Federal Register information and research tools, including Public Inspection List and electronic text are located at: www.federalregister.gov.

E-mail

FEDREGTOC (Daily Federal Register Table of Contents Electronic Mailing List) is an open e-mail service that provides subscribers with a digital form of the Federal Register Table of Contents. The digital form of the Federal Register Table of Contents includes HTML and PDF links to the full text of each document.

To join or leave, go to <https://public.govdelivery.com/accounts/USGPOOFR/subscriber/new>, enter your email address, then follow the instructions to join, leave, or manage your subscription.

PENS (Public Law Electronic Notification Service) is an e-mail service that notifies subscribers of recently enacted laws.

To subscribe, go to <http://listserv.gsa.gov/archives/publaws-l.html> and select *Join or leave the list (or change settings)*; then follow the instructions.

FEDREGTOC and **PENS** are mailing lists only. We cannot respond to specific inquiries.

Reference questions. Send questions and comments about the Federal Register system to: fedreg.info@nara.gov

The Federal Register staff cannot interpret specific documents or regulations.

FEDERAL REGISTER PAGES AND DATE, APRIL

22327-22606.....	1
22607-22878.....	2
22879-23496.....	3
23497-23906.....	4

CFR PARTS AFFECTED DURING APRIL

At the end of each month the Office of the Federal Register publishes separately a List of CFR Sections Affected (LSA), which lists parts and sections affected by documents published since the revision date of each title.

3 CFR	
Executive Orders:	
14121.....	22327
Proclamations:	
10714.....	22879
10715.....	22881
10716.....	22883
10717.....	22885
10718.....	22887
10719.....	22889
10720.....	22891
10721.....	22893
10722.....	22895
10723.....	22899
10724.....	22901
10725.....	23497
6 CFR	
3.....	23499
Proposed Rules:	
226.....	23644
7 CFR	
301.....	23500
8 CFR	
103.....	22607
214.....	22903
235.....	22607
258.....	23501
1003.....	22630
9 CFR	
441.....	22331
10 CFR	
30.....	22636
40.....	22636
50.....	22912
52.....	22912
70.....	22636
430.....	22914
14 CFR	
25.....	23504, 23507
39.....	22333, 22925, 22928, 22932
61.....	22482
63.....	22482
65.....	22482
71.....	23510
97.....	22334, 22336
Proposed Rules:	
39.....	22356, 22358, 22640, 23529
71.....	22362, 22642, 23532
15 CFR	
732.....	23876
734.....	23876
736.....	23876
16 CFR	
Proposed Rules:	
305.....	22644
24 CFR	
115.....	22934
125.....	22934
26 CFR	
54.....	23338
Proposed Rules:	
1.....	22971
54.....	22971
301.....	22971
29 CFR	
1903.....	22558
2550.....	23090
2590.....	23338
Proposed Rules:	
2510.....	22971
2520.....	22971
2550.....	22971
4000.....	22971
4007.....	22971
4010.....	22971
4041.....	22971
4041A.....	22971
4043.....	22971
4050.....	22971
4062.....	22971
4063.....	22971
4204.....	22971
4211.....	22971
4219.....	22971
4231.....	22971
4245.....	22971
4262.....	22971
4281.....	22971
33 CFR	
1.....	22942
5.....	22942
104.....	22942
151.....	22942
155.....	22942
161.....	22942
164.....	22942
165.....	22637, 22942, 23512
174.....	22942
175.....	22942
Proposed Rules:	
165.....	22645

34 CFR	63.....23294, 23840	418.....23778	48 CFR
Ch. VI.....23514	75.....23526	488.....23424	Ch. 1.....22604, 22605
36 CFR	78.....23526		40.....22604
242.....22949	97.....23526	45 CFR	519.....22638
37 CFR	Proposed Rules:	144.....23338	538.....22966
	52.....22363, 22648	146.....23338	552.....22638, 22966
	751.....22972	148.....23338	
Proposed Rules:	42 CFR	46 CFR	50 CFR
1.....23226	431.....22780	3.....22942	17.....22522
41.....23226	435.....22780	15.....22942	100.....22949
42.....23226	436.....22780	70.....22942	300.....22966
38 CFR	447.....22780	117.....22942	660.....22342, 22352
17.....23518	457.....22780	118.....22942	Proposed Rules:
40 CFR	600.....22780	119.....22942	17.....22649, 23534
52.....22337, 22963, 23521,	Proposed Rules:	147.....22942	679.....23535
23523, 23526	412.....23146	47 CFR	
	413.....23424	2.....23527	

LIST OF PUBLIC LAWS

Note: No public bills which have become law were received by the Office of the Federal Register for inclusion

in today's **List of Public Laws**.

Last List March 26, 2024

Public Laws Electronic Notification Service (PENS)

PENS is a free email notification service of newly

enacted public laws. To subscribe, go to https://portalguard.gsa.gov/__layouts/PG/register.aspx.

Note: This service is strictly for email notification of new laws. The text of laws is not available through this service. **PENS** cannot respond to specific inquiries sent to this address.