

than 5:00 p.m. EST on January 12, 2016. Comments received after January 12, 2016, will be distributed to the Committee, but may not be considered at the meetings. The minutes of the meetings will be posted on the Committee Web site within 60 days of the meeting.

Dated: December 7, 2015.

David Long,

Director, Office of Supply Chain and Professional & Business Services.

[FR Doc. 2015-31195 Filed 12-10-15; 8:45 am]

BILLING CODE 3510-DR-P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket Number: 151103999-5999-01]

Views on the Framework for Improving Critical Infrastructure Cybersecurity

ACTION: Notice; Request for Information (RFI).

SUMMARY: The National Institute of Standards and Technology (NIST) is seeking information on the “Framework for Improving Critical Infrastructure Cybersecurity” (the “Framework”).

As directed by Executive Order 13636, “Improving Critical Infrastructure Cybersecurity” (the “Executive Order”), the Framework consists of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Framework was released on February 12, 2014, after a year-long open process involving private and public sector organizations, including extensive industry input and public comments. In order to fulfill its responsibilities under the Cyber Security Enhancement Act of 2014, NIST is committed to maintaining an inclusive approach, informed by the views of a wide array of individuals, organizations, and sectors.

In this RFI, NIST requests information about the variety of ways in which the Framework is being used to improve cybersecurity risk management, how best practices for using the Framework are being shared, the relative value of different parts of the Framework, the possible need for an update of the Framework, and options for the long-term governance of the Framework. This information is needed in order to carry out NIST’s responsibilities under the Cybersecurity Enhancement Act of 2014 and the Executive Order.

Responses to this RFI—which will be posted at <http://www.nist.gov/cyberframework/cybersecurity->

[framework-rfi.cfm](http://www.nist.gov/cyberframework/rfi.cfm)—will inform NIST’s planning and decision-making about how to further advance the Framework so that the Nation’s critical infrastructure is more secure by enhancing its cybersecurity and risk management.

All information provided will also assist in developing the agenda for a workshop on the Framework being planned by NIST for April 6 and 7, 2016, in Gaithersburg, Maryland. Specifics about the workshop will be announced at a later date.

DATES: Comments must be received by 5:00 p.m. Eastern time on February 9, 2016.

ADDRESSES: Written comments may be submitted by mail to Diane Honeycutt, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899. Online submissions in electronic form may be sent to cyberframework@nist.gov in any of the following formats: HTML; ASCII; Word; RTF; or PDF. Please include your name and your organization’s name (if any), and cite “Views on the Framework for Improving Critical Infrastructure Cybersecurity” in all correspondence. Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials. Please do not submit additional materials.

All comments received in response to this RFI will be posted at <http://www.nist.gov/cyberframework/cybersecurity-framework-rfi.cfm> without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information).

FOR FURTHER INFORMATION CONTACT: For questions about this RFI contact: Diane Honeycutt, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899 or cyberframework@nist.gov. Please direct media inquiries to NIST’s Office of Public Affairs at (301) 975-2762.

SUPPLEMENTARY INFORMATION: NIST is authorized by the Cybersecurity Enhancement Act of 2014¹ to “facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure.”²

¹ Public Law 113-274 (2014): <http://www.gpo.gov/fdsys/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf>.

² *Id.*, codified in relevant part at 15 U.S.C. 272(c)(15). Congress’s intent was to codify NIST’s

role in Executive Order No. 13636: “Title I would codify certain elements of Executive Order 13636 by directing the National Institute of Standards and Technology (NIST) to develop a framework of voluntary standards designed to reduce risks arising from cyberattacks on critical infrastructure that is privately owned and operated.” S. Rep. No. 113-270, at 9 (2014).

role in Executive Order No. 13636: “Title I would codify certain elements of Executive Order 13636 by directing the National Institute of Standards and Technology (NIST) to develop a framework of voluntary standards designed to reduce risks arising from cyberattacks on critical infrastructure that is privately owned and operated.” S. Rep. No. 113-270, at 9 (2014).

³ *Id.*, codified in relevant part at 15 U.S.C. 272(e)(A)(i).

⁴ Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 FR 11739 (Feb. 19, 2013).

⁵ NIST, Gaithersburg April 3, 2013; Carnegie Mellon University May 29–31, 2013; University of California San Diego July 10–12, 2013; University of Texas Dallas September 11–13, 2013; North Carolina State November 14–15, 2013.

In carrying out this function, NIST is directed to “coordinate closely and regularly with relevant private sector personnel and entities, critical infrastructure owners and operators, and other relevant industry organizations.”³ NIST has taken this approach since February 2013 when Executive Order 13636, “Improving Critical Infrastructure Cybersecurity”⁴ tasked the Secretary of Commerce to direct the Director of NIST to lead the development of the Framework. NIST developed the Framework by using information collected through a Request for Information (RFI) that was published in the **Federal Register** (78 FR 13024) on February 26, 2013; a series of five open public workshops;⁵ and a 45-day public comment period in response to a draft version of the Framework announced in the **Federal Register** (78 FR 64478) on October 29, 2013. A final version of Framework 1.0 was published on February 12, 2014, after a year-long, open process involving private and public sector organizations, including extensive industry input and public comments, and announced in the **Federal Register** (79 FR 9167) on February 18, 2014. NIST subsequently solicited information on Framework users’ experiences through an RFI published in the **Federal Register** (79 FR 50891) on August 26, 2014 as well as another workshop held on October 29 and 30, 2014, at the University of South Florida.

In addition to extensive outreach and providing responses to inquiries, NIST has made information about the Cybersecurity Framework available on its Web site at <http://www.nist.gov/cyberframework/> to assist organizations in learning more about using the Framework. This includes an Industry Resources page (available at <http://www.nist.gov/cyberframework/cybersecurity-framework-industry-resources.cfm>), listing publicly available materials developed by organizations other than NIST that support use of the Framework. NIST does not necessarily

role in Executive Order No. 13636: “Title I would codify certain elements of Executive Order 13636 by directing the National Institute of Standards and Technology (NIST) to develop a framework of voluntary standards designed to reduce risks arising from cyberattacks on critical infrastructure that is privately owned and operated.” S. Rep. No. 113-270, at 9 (2014).

³ *Id.*, codified in relevant part at 15 U.S.C. 272(e)(A)(i).

⁴ Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 FR 11739 (Feb. 19, 2013).

⁵ NIST, Gaithersburg April 3, 2013; Carnegie Mellon University May 29–31, 2013; University of California San Diego July 10–12, 2013; University of Texas Dallas September 11–13, 2013; North Carolina State November 14–15, 2013.

endorse, approve, or recommend any of the commercial entities, equipment, or materials listed on the Industry Resources page, nor does it imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Since the Framework's release as version 1.0, NIST has continued to work on topics raised during the Framework's development but not integrated into version 1.0 of the Framework. These are listed in the NIST Roadmap for Improving Critical Infrastructure Cybersecurity. Significant progress has been made in several of these areas, through programs like the National Initiative for Cybersecurity Education and the National Strategy for Trusted Identities in Cyberspace.

Request for Information

Continuing its inclusive approach, in advance of any decision regarding possible updates of the Framework and Framework stewardship, NIST is interested in hearing from all stakeholders.⁶

In this RFI, NIST seeks specific information about the variety of ways in which the Framework is being used and the relative value of different parts of the Framework, the possible need for an update of the Framework, how best practices for using the Framework are being shared and might be enhanced, and the long-term governance of Framework. This information is needed to carry out NIST's statutory responsibilities with the ultimate goal of assisting organizations as they seek to improve their cybersecurity risk management practices.

Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials. Do not include in comments or otherwise submit proprietary or confidential information, as all comments received in response to this RFI will be made available publicly at <http://www.nist.gov/cyberframework/cybersecurity-framework-rfi.cfm>.

Respondents may organize their submissions in response to this RFI

⁶The Cybersecurity Enhancement Act of 2014, Public Law 113-274 (2014), codified in relevant part at 15 U.S.C. 272(e)(A)(i) and 272(e)(A)(ii) specifically calls for NIST to "coordinate closely and regularly with relevant private sector personnel and entities, critical infrastructure owners and operators, and other relevant industry organizations, including Sector Coordinating Councils and Information Sharing and Analysis Centers, and incorporate industry expertise" and to "consult with the heads of agencies with national security responsibilities, sector-specific agencies and other appropriate agencies, State and local governments, the governments of other nations, and international organizations."

using the template available at <http://www.nist.gov/cyberframework/cybersecurity-framework-rfi.cfm>. Use of this template is not required and all responses that comply with the requirements listed in the **ADDRESSES** and **DATES** section of this notice will be considered whether or not the template is used.

While the Framework and associated outreach activities by NIST have focused on critical infrastructure, this RFI generally uses the broader term "organizations" in seeking information.

The following questions cover the major areas about which NIST seeks comment. They are not intended to limit the topics that may be addressed. Responses may include any topic believed to have implications for the voluntary use and subsequent improvement of the Framework, regardless of whether the topic is included in this document.

Use of the Framework

1. Describe your organization and its interest in the Framework.
2. Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.
3. If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).
4. What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?
5. What portions of the Framework are most useful?
6. What portions of the Framework are least useful?
7. Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?
8. To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.
9. What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?⁷

⁷*Id.*, codified in relevant part at 15 U.S.C. 272(e)(1)(A)(vii).

Possible Framework Updates

10. Should the Framework be updated? Why or why not?

11. What portions of the Framework (if any) should be changed or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.

12. Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?

13. Are there approaches undertaken by organizations—including those documented in sector-wide implementation guides—that could help other sectors or organizations if they were incorporated into the Framework?

14. Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap"⁸ be used to inform any updates to the Framework? If so, how?

15. What is the best way to update the Framework while minimizing disruption for those currently using the Framework?

Sharing Information on Using the Framework

16. Has information that has been shared by NIST or others affected your use of the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?

17. What, if anything, is inhibiting the sharing of best practices?

18. What steps could the U.S. government take to increase sharing of best practices?

19. What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?

Private Sector Involvement in the Future Governance of the Framework

20. What should be the private sector's involvement in the future governance of the Framework?

21. Should NIST consider transitioning some or even all of the

⁸NIST Roadmap for Improving Critical Infrastructure Cybersecurity (February 12, 2014), Roadmap areas for Development, Alignment, and Collaboration include: Authentication; automated indicator sharing; conformity assessment; cybersecurity workforce; data analytics; federal agency cybersecurity alignment; international aspects, impacts, and alignment; supply chain risk management; and technical privacy standards. <http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf>.

Framework's coordination to another organization?

22. If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?

23. If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?

24. How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?

25. What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?

Richard Cavanagh,

Acting Associate Director for Laboratory Programs.

[FR Doc. 2015-31217 Filed 12-10-15; 8:45 am]

BILLING CODE 3510-13-P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Proposed Information Collection; Comment Request; Permit and Reporting Requirements for Non-Commercial Fishing in the Rose Atoll, Marianas Trench, and Pacific Remote Islands Marine National Monuments

AGENCY: National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice.

SUMMARY: The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995.

DATES: Written comments must be submitted on or before February 9, 2016.

ADDRESSES: Direct all written comments to Jennifer Jessup, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6616, 14th and Constitution Avenue NW., Washington, DC 20230 (or via the Internet at Jjessup@doc.gov).

FOR FURTHER INFORMATION CONTACT:

Direct requests for additional information or copies of the information collection instrument and instructions to Walter Ikehara, (808) 725-5175 or Walter.Ikehara@noaa.gov.

SUPPLEMENTARY INFORMATION:

I. Abstract

This request is for extension of a current information collection.

The National Marine Fisheries Service (NMFS) manages fishing activities in the Rose Atoll Marine, Marianas Trench, and Pacific Remote Islands Marine National Monuments. Regulations at 50 CFR part 665 require the owner and operator of a vessel used to non-commercially fish for, take, retain, or possess any management unit species in these monuments to hold a valid permit.

Regulations also require the owner and operator of a vessel that is chartered to fish recreationally for, take, retain, or possess, any management unit species in these monuments to hold a valid permit. The fishing vessel must be registered to the permit. The charter business must be established legally in the permit area where it will operate. Charter vessel clients are not required to have a permit.

The permit application collects basic information about the permit applicant, type of operation, vessel, and permit area. NMFS uses this information to determine permit eligibility. The information is important for understanding the nature of the fishery and provides a link to participants. It also aids in the enforcement of Fishery Ecosystem Plan measures.

Regulations also require the vessel operator to report a complete record of catch, effort, and other data on a NMFS logsheet. The vessel operator must record all requested information on the logsheet within 24 hours of the completion of each fishing day. The vessel operator also must sign, date, and submit the form to NMFS within 30 days of the end of each fishing trip.

II. Method of Collection

NMFS collects information on paper permit applications and logsheets.

III. Data

OMB Control Number: 0648-0664.

Form Number(s): None.

Type of Review: Regular (extension of a currently approved information collection).

Affected Public: Business or other for-profit organizations, individuals or households.

Estimated Number of Respondents: 25.

Estimated Time per Response: 15 minutes per permit application; 20 minutes per logsheet form.

Estimated Total Annual Burden Hours: 40.

Estimated Total Annual Cost to Public: \$100 in recordkeeping/reporting costs.

IV. Request for Comments

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 (including hours and cost) of the proposed collection of information; (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 respondents, including through the use of automated collection techniques or other forms of information technology.

Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval of this information collection; they also will become a matter of public record.

Dated: December 7, 2015.

Sarah Brabson,

NOAA PRA Clearance Officer.

[FR Doc. 2015-31164 Filed 12-10-15; 8:45 am]

BILLING CODE 3510-22-P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648-XD065

Takes of Marine Mammals Incidental to Specified Activities; Taking Marine Mammals Incidental to Murray Street Bridge Seismic Retrofit Project by the California State Department of Transportation

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice; proposed incidental harassment authorization; request for comments and information.

SUMMARY: NMFS has received an application from California State Department of Transportation (Caltrans) for an Incidental Harassment Authorization (IHA) to take marine mammals, by harassment, incidental to Murray Street Bridge seismic retrofit project in Santa Cruz, California.