U.S. GOVERNMENT PUBLISHING OFFICE

Government Publishing and Print Procurement

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

MEDICARE (Part D Subsidy) NOTICES

as requisitioned from the U.S. Government Publishing Office (GPO) by the

Social Security Administration (SSA)

Single Award

TERM OF CONTRACT: The term of this contract is for the period beginning March 1, 2027 and ending February 29, 2028, plus up to four (4) optional 12-month extension periods that may be added in accordance with the "OPTION TO EXTEND THE TERM OF THE CONTRACT" clause in SECTION 1 of this contract.

The period from March 1, 2027 through August 31, 2027, will be used by the contractor for testing and interfacing with SSA's National File Transfer Management System (FTMS) for electronic transmission of files from SSA to the production facility. Live production begins on September 1, 2027.

BID OPENING: Bids shall be opened virtually at 11:00 a.m., Eastern Time (ET), on November 19, 2026, at the U.S. Government Publishing Office. All parties interested in attending the bid opening shall email bids@gpo.gov one (1) hour prior to the bid opening date and time to request a Microsoft Teams live stream link. This must be a separate email from the bid submission. The link will be emailed prior to the bid opening.

BID SUBMISSION: Bidders must email bids to bids@gpo.gov for this solicitation. No other method of bid submission will be accepted at this time. The program number and bid opening date must be specified in the subject line of the emailed bid submission. ***Bids received after the bid opening date and time specified above will not be considered for award.***

RESTRICTION ON LOCATION OF PRODUCTION FACILITIES: Due to the security requirements set forth in these specifications, this program must be produced in the continental United States*.

* See clause defining the "United States" in the "SSA EXTERNAL SERVICE PROVIDER SECURITY REQUIREMENTS".

BIDDERS, PLEASE NOTE: ***This program was formerly Program 272-S.*** These specifications have been extensively revised; therefore, all bidders are cautioned to familiarize themselves with all provisions of these specifications before bidding, with particular attention to:

- All security requirements/clauses/specifications specified in SECTION 1.
- SECTION 2. – Preproduction Tests, Proofs, Printing and Imaging, Distribution

Abstracts of contract prices are available at https://www.gpo.gov/how-to-work-with-us/vendors/contract-pricing.

For information of a technical nature, contact Traci Cobb at tcobb@gpo.gov or (202) 512-0424.

SECTION 1. – GENERAL TERMS AND CONDITIONS

GPO CONTRACT TERMS: Any contract which results from this Invitation for Bid will be subject to the applicable provisions, clauses, and supplemental specifications of GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987 (Rev. 01-18)) and GPO Contract Terms, Quality Assurance through Attributes Program for Printing and Binding (GPO Publication 310.1, effective May 1979 (Rev. 09-19)).

GPO Contract Terms (GPO Publication 310.2) – https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/contractterms2018.pdf.

GPO QATAP (GPO Publication 310.1) – https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/qatap-rev-09-19.pdf.

SUBCONTRACTING: The predominant production functions are the printing of notices, the laser/ion deposition printing/imaging of data at a minimum of 600 x 600 dpi for the notices from electronically transmitted files, folding, inserting, presorting, mailing, and disposal of waste materials. Any bidder who cannot perform the predominant production functions of this contract will be declared non-responsible. (***Inkjet printing is not allowed.***)

Contractor may subcontract the printing and manufacturing of the envelopes.

The contractor is responsible for enforcing all contract requirements outsourced to a subcontractor.

If the contractor needs to add a subcontractor at any time after award, the subcontractor must be approved by the Government prior to production starting in that facility. If the subcontractor is not approved by the Government, then the contractor must submit new subcontractor's information to the Government for approval 30 calendar days prior to the start of production at that facility.

QUALITY ASSURANCE LEVELS AND STANDARDS: The following levels and standards shall apply to these specifications:

Product Quality Levels:

(a) Printing Attributes – Level III.
(b) Finishing Attributes – Level III.

Inspection Levels (from ANSI/ASQC Z1.4):

(a) Non-destructive Tests - General Inspection Level I.
(b) Destructive Tests - Special Inspection Level S-2.
(c) Transparent, low-gloss, poly-type window material, covering the envelope window, must pass a readability test with a rejection rate of less than 1/4% of 1% when run through a U.S. Postal Service (USPS) OCR scanner.
(d) Exception: ANSIX3.17 "Character Set for Optical Character Recognition (OCR-A)" shall apply to these specifications. The revisions of this standard are effective as of the date of this contract are those which shall apply.
(e) Exception: The PDF417 (Portable Data File) 2D barcodes must be in accordance with the requirements of ANSI MH 10.8.3M unless otherwise specified.

ANSI Standards may be obtained from the American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036.

Specified Standards: The specified standards for the attributes requiring them shall be:

Attribute	Specified Standard
P-7. Type Quality and Uniformity	O.K. Press Sheets

Special Instructions: In the event the inspection of press sheets is waived by the Government, the following list of alternate standards (in order of precedence) shall become the Specified Standards:

P-7. O.K. Press Samples; Average Type Dimension.

NOTE: The scannable forms produced under these specifications must be guaranteed to function properly when processed through the high-speed scanner equipment at SSA. SSA will be using Top Image Systems scanning software to process the images and OCR engines to do the OCR/ICR recognition. The 2D barcodes will be read during scanning by proprietary software from the scanner manufacturer.

OPTION TO EXTEND THE TERM OF THE CONTRACT: The Government has the option to extend the term of this contract for a period of 12 months by written notice to the contractor not later than 30 days before the contract expires. If the Government exercises this option, the extended contract shall be considered to include this clause, except, the total duration of the contract may not exceed five (5) years as a result of, and including, any extension(s) added under this clause. Further extension may be negotiated under the "EXTENSION OF CONTRACT TERM" clause. See also "ECONOMIC PRICE ADJUSTMENT" for authorized pricing adjustment(s).

EXTENSION OF CONTRACT TERM: At the request of the Government, the term of any contract resulting from this solicitation may be extended for such period of time as may be mutually agreeable to the GPO and the contractor.

ECONOMIC PRICE ADJUSTMENT: The pricing under this contract shall be adjusted in accordance with this clause, provided that in no event will any pricing adjustment be made that would exceed the maximum permissible under any law in effect at the time of the adjustment. There will be no adjustment for orders placed during the first period specified below. Pricing will thereafter be eligible for adjustment during the second and any succeeding performance period(s). For each performance period after the first, a percentage figure will be calculated as described below and that figure will be the economic price adjustment for that entire next period. Pricing adjustments under this clause are not applicable to reimbursable postage or transportation costs, or to paper, if paper prices are subject to adjustment by separate clause elsewhere in this contract.

For the purpose of this clause, performance under this contract will be divided into successive periods. The first period will extend from March 1, 2027 to February 29, 2028 and the second and any succeeding period(s) will extend for 12 months from the end of the last preceding period, except that the length of the final period may vary. The first day of the second and any succeeding period(s) will be the effective date of the economic price adjustment for that period.

Pricing adjustments in accordance with this clause will be based on changes in the seasonally adjusted "Consumer Price Index For All Urban Consumers – Commodities less Food" (Index) published monthly in the CPI Detailed Report by the U.S. Department of Labor, Bureau of Labor Statistics.

The economic price adjustment will be the percentage difference between Index averages as specified in this paragraph. An index called the variable index will be calculated by averaging the monthly Indexes from the 12-month interval ending three (3) months prior to the beginning of the period being considered for adjustment. This average is then compared to the average of the monthly Indexes for the 12-month interval ending November 30, 2026, called the base index. The percentage change (plus or minus) of the variable index from the base index will be the economic price adjustment for the period being considered for adjustment.

The Government will notify the contractor by contract modification specifying the percentage increase or decrease to be applied to invoices for orders placed during the period indicated. The contractor shall apply the percentage increase or decrease against the total price of the invoice less reimbursable postage or transportation costs and separately adjusted paper prices. Payment discounts shall be applied after the invoice price is adjusted.

PAPER PRICE ADJUSTMENT: Paper prices charged under this contract will be adjusted in accordance with "Table 9 - Producer Price Indexes and Percent Changes for Commodity Groupings and Individual Items" in Producer Price Indexes report, published by the Bureau of Labor Statistics (BLS), as follows:

NOTE: For the purpose of this contract, the Paper Price Adjustment will be based on the date of actual production. Actual live production begins September 1, 2027.

1. BLS code 0913-01 for Offset and Text will apply to all paper required under this contract.

2. The applicable index figures for the month of August 2027 will establish the base index.

3. There shall be no price adjustment for the first three (3) production months of the contract.

4. Price adjustments may be monthly thereafter, but only if the index varies by an amount (plus or minus) exceeding 5% by comparing the base index to the index for that month, which is two months prior to the month being considered for adjustment.

5. Beginning with order placement in the fourth month, index variances will be calculated in accordance with the following formula:

$$\frac{X - \text{Base Index}}{\text{Base Index}} \times 100 = _____ \%$$

   where X = the index for that month which is two months prior to the month being considered for adjustment.

6. The contract adjustment amount, if any, will be the percentage calculated in 5 above less 5%.

7. Adjustments under this clause will be applied to the contractor's bid price(s) for Item VI., "PAPER" in the "SCHEDULE OF PRICES" and will be effective on the first day of any month for which prices are to be adjusted.

The Contracting Officer will give written notice to the contractor of any adjustments to be applied to invoices for orders placed during months affected by this clause.

In no event, however, will any price adjustment be made which would exceed the maximum permissible under any law in effect at the time of the adjustment. The adjustment, if any, shall not be based upon the actual change in cost to the contractor, but shall be computed as provided above.

The contractor warrants that the paper prices set forth in this contract do not include any allowance for any contingency to cover anticipated increased costs of paper to the extent such increases are covered by this price adjustment clause.

SECURITY REQUIREMENTS: Clause 2352.224-1 Protection of Confidential Information (Dec 2008):

(a) "Confidential information," as used in this clause, means information or data, or copies or extracts of information or data, that is: (1) provided by the Social Security Administration (SSA) to the contractor for, or otherwise obtained by the contractor in, the performance of this contract; and (2) of a personal nature about an individual, such as name, home address, and social security number, or proprietary information or data submitted by or pertaining to an institution or organization, such as employee pay scales and indirect cost rates.

(b) The Contracting Officer and the contractor may, by mutual consent, identify elsewhere in this contract specific information or categories of information that the Government will furnish to the contractor or that the contractor is expected to generate which are confidential. Similarly, the Contracting Officer and the contractor may, by mutual consent, identify such confidential information from time to time during the performance of the contract. The confidential information will be used only for purposes delineated in the contract; any other use of the confidential information will require the Contracting Officer's express written authorization. The Contracting Officer and the contractor will settle any disagreements regarding the identification pursuant to the "Disputes" clause.

(c) The contractor shall restrict access to all confidential information to the minimum number of employees and officials who need it to perform the contract. Employees and officials who need access to confidential information for performance of the contract will be determined in conference between SSA's Contracting Officer, Contracting Officer's Technical Representative, and the responsible contractor official. Upon request, the contractor will provide SSA with a list of "authorized personnel," that is, all persons who have or will have access to confidential information covered by this clause.

(d) The contractor shall process all confidential information under the immediate supervision and control of authorized personnel in a manner that will: protect the confidentiality of the records; prevent the unauthorized use of confidential information; and prevent access to the records by unauthorized persons.

(e) The contractor shall assure that each contractor employee with access to confidential information knows the prescribed rules of conduct, and that each contractor employee is aware that he/she may be subject to criminal penalties for violations of the Privacy Act and/or the Social Security Act.

When the contractor employees are made aware of this information, they will be required to sign the SSA-301, "Contractor Personnel Security Certification" (see Exhibit A).

A copy of this signed certification must be forwarded to: Social Security Administration, Attn: Melissa Picone, Printing and Postage, 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401, or email to: melissa.picone@ssa.gov. A copy must also be forwarded to: U.S. Government Publishing Office, Attn: Traci Cobb (tcobb@gpo.gov). (See paragraph (f) below regarding the minimum standards that the safeguards must meet.)

(f) Whenever the contractor is storing, viewing, transmitting, or otherwise handling confidential information, the contractor shall comply with the applicable standards for security controls that are established in the Federal Information Security Modernization Act (FISMA). (These standards include those set by the National Institute of Standards and Technology (NIST) via the Federal Information Processing Standards (FIPS) publications and NIST Special Publications, particularly FIPS 199, FIPS 200, and NIST Special Publications - 800 series.)

(g) If the contractor, in the performance of the contract, uses any information subject to the Privacy Act of 1974, 5 U.S.C. 552a, and/or section 1106 of the Social Security Act, 42 U.S.C. 1306, the contractor must follow the rules and procedures governing proper use and disclosure set forth in the Privacy Act, section 1106 of the Social Security Act, and the Commissioner's regulations at 20 C.F.R. Part 401 with respect to that information.

(h) For knowingly disclosing information in violation of the Privacy Act, the contractor and contractor employees may be subject to the criminal penalties as set forth in 5 U.S.C. Section 552(i)(1) to the same extent as employees of SSA. For knowingly disclosing confidential information as described in section 1106 of the Social Security Act (42 U.S.C. 1306), the contractor and contractor employees may be subject to the criminal penalties as set forth in that provision.

(i) The contractor shall assure that each contractor employee with access to confidential information is made aware of the prescribed rules of conduct and the criminal penalties for violations of the Privacy Act and/or the Social Security Act.

(j) Whenever the contractor is uncertain how to handle properly any material under the contract, the contractor must obtain written instructions from the Contracting Officer addressing this question. If the material in question is subject to the Privacy Act and/or section 1106 of the Social Security Act or is otherwise confidential information subject to the provisions of this clause, the contractor must obtain a written determination from the Contracting Officer prior to any release, disclosure, dissemination, or publication. Contracting Officer instructions and determinations will reflect the result of internal coordination with appropriate program and legal officials.

(k) Performance of this contract may involve access to tax return information as defined in 26 U.S.C. Section 6103(b) of the Internal Revenue Code (IRC). All such information shall be confidential and may not be disclosed without the written permission of the SSA Contracting Officer. For willingly disclosing confidential tax return information in violation of the IRC, the contractor and contractor employees may be subject to the criminal penalties set forth in 26 U.S.C. Section 7213. (Refer to "SAFEGUARDING FEDERAL TAX INFORMATION REQUIREMENTS.")

(l) The SSA reserves the right to conduct on-site visits to review the contractor's documentation and in-house procedures for protection of and security arrangements for confidential information and adherence to the terms of this clause.

(m) The SSA reserves the right to inspect contractor facilities to ensure compliance with this contract. If facilities are found deficient, the contractor must implement corrective actions within 45 calendar days of notification.

(n) The contractor must include this clause in all resulting subcontracts whenever there is any indication that the subcontractor(s), engaged by the contractor, and their employees or successor subcontractor(s) and their employees might have access to SSA's confidential information.

(o) The contractor must assure that its subcontractor(s) and their employees or any successor subcontractor(s) and their employees with access to SSA confidential information are made aware of the prescribed rules of conduct. For knowingly disclosing SSA's confidential information, any subcontractor(s) and their employees or successor subcontractor(s) and their employees may be subject to criminal penalties as described in section 1106 of the Social Security Act (42 U.S.C. 1306) and the Privacy Act (5 U.S.C. 552a).

SSA EXTERNAL SERVICE PROVIDER SECURITY REQUIREMENTS: This resource identifies the basic information security requirements related to the procurement of Information Technology (IT) services hosted externally to SSA's Network.

The following general security requirements apply to all External Service Providers (ESP):

a. The solution must be located in the United States, its territories, or possessions.

NOTE: "United States" means the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, Johnston Island, Wake Island, and Outer Continental Shelf Lands as defined in the Outer Continental Shelf Lands Act (43 U.S.C. 1331, et seq.), but does not include any other place subject to U.S. jurisdiction or any U.S. base or possession within a foreign country (29 CFR 4.112).

b. Upon request from the SSA Contracting Officer Technical Representative (COTR), the ESP shall provide access to the hosting facility to the U.S. Government or authorized agents for inspection and facilitate an on-site security risk and vulnerability assessment.

c. The solution must meet Federal Information Processing Standards (FIPS) and guidance developed by the National Institute of Science and Technology (NIST) under its authority provided by the Federal Information Security Modernization Act (FISMA) to develop security standards for federal information processing systems, and Office of Management and Budget's (OMB) Circular A-130 Appendix III.

d. ESPs classified as Cloud Service Providers (CSP) must be FedRAMP authorized. As part of these requirements, CSPs must have a security control assessment performed by a Third Party Assessment Organization (3PAO).

e. The ESP shall submit to the SSA COTR documentation describing how the solution implements security controls in accordance with the designated categorization (FIPS 199) and the Minimum Security Requirements for Federal Information and Information Systems (FIPS 200) which requires the use of NIST SP 800-53r5 (or later) before SSA provides data.

f. All ESPs that process or store Personally Identifiable Information (PII) (as defined in Clause 2352.224-2A (a)) are considered a Moderate impact categorization. If PII or sensitive data (defined by the COTR) is stored or processed by the ESP, then the ESP shall provide a Security Authorization Package (SAP), which will undergo a Triannual Full Assessment and will undergo an Annual Review. The SAP should include a System Security Plan (SSP), Security Assessment Report (SAR), Risk Assessment Report (RAR), and Plan of Action & Milestone Report (POA&M). The SAP must be reviewed by SSA before the SSA transfers data to the ESP. Refer to NIST SP 800-37 and NIST SP 800-53r5 (or later) for more information on the Security Authorization Package. (Refer to "SAFEGUARDING FEDERAL TAX INFORMATION REQUIREMENTS" if an independent assessor is needed to accomplish this requirement.)

NOTE: Independent assessor is any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system.

g. SSA will consider a self-assessment of security controls for solutions that do not involve sensitive information or PII.

References - Contractor must comply with latest version in effect for the following documents and publications:

- Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.govinfo.gov/app/details/PLAW-113publ283

- Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996." https://www.govinfo.gov/content/pkg/USCODE-2011-title40/html/USCODE-2011-title40-subtitleIII.htm

- Privacy Act (P.L. 93-579), December 1974. https://www.govinfo.gov/app/details/STATUTE-88/STATUTE-88-Pg1896

- Homeland Security Presidential Directive 12 (HSPD-12): "Policy for a Common Identification Standard for Federal Employees and Contractors," January 27, 2022. https://www.dhs.gov/homeland-security-presidential-directive-12

- Revision of OMB Circular No. A–130, "Managing Information as a Strategic Resource," July 28, 2016. https://www.govinfo.gov/content/pkg/FR-2016-07-28/pdf/2016-17872.pdf

- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," December 16, 2003. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf

- ITL BULLETIN FOR DECEMBER 2011 REVISED GUIDELINE FOR ELECTRONIC AUTHENTICATION OF USERS HELPS ORGANIZATIONS PROTECT THE SECURITY OF THEIR INFORMATION SYSTEMS. https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul2011-12.pdf

- FIPS PUB 199, National Institute of Standards and Technology, Federal Information Processing Standards Publication, "Standards for Security Categorization of Federal Information and Information Systems," February 2004. https://doi.org/10.6028/NIST.FIPS.199

- FIPS PUB 200, National Institute of Standards and Technology, Federal Information Processing Standards Publication, "Minimum Security Requirements for Federal Information and Information Systems," March 2006. https://doi.org/10.6028/NIST.FIPS.200

- FIPS 140-3, "Security Requirements for Cryptographic Modules," March 22, 2019. https://csrc.nist.gov/publications/detail/fips/140/3/final

- NIST Special Publication (SP) 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems," February 2006. https://doi.org/10.6028/NIST.SP.800-18r1

- NIST SP 800-30, Revision 1, "Guide for Conducting Risk Assessments," September 2012. https://doi.org/10.6028/NIST.SP.800-30r1

- NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems," November 2010. https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2010-07.pdf

- NIST SP 800-37, Rev. 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

- NIST SP 800-47, Rev. 1, "Managing the Security of Information Exchanges," July 2021. https://csrc.nist.gov/News/2021/nist-publishes-sp-800-47-rev-1

- NIST SP 800-53, Rev. 5, "Security and Privacy Controls for Information Systems and Organizations," September 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

- NIST SP 800-53A, Revision 5, "Assessing Security and Privacy Controls in Information Systems and Organizations," January 2022.
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf

- NIST SP 800-60, Vol. 1, Rev. 1, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008.
  https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final

- NIST SP 800-60, Vol. 2 Rev. 1, "Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices," August 2008.
  https://csrc.nist.gov/publications/detail/sp/800-60/vol-2-rev-1/final

- OMB M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 2017.

- NIST 800-171, Rev. 3, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," May 2024.
  https://csrc.nist.gov/pubs/sp/800/171/r3/final

With the everchanging security models and requirements, OIS recommends that the contractor formally request updated templates and requirement changes via email annually from the date of the award.

The publications specified below contain current examples of templates. The contractor will need to evaluate the templates and complete them as appropriate. Additional guidance can be found from the NIST links above. The contractor will need to work with SSA to determine if the 800-53r5 or 800-171r3 SSP templates should be used, or if there are new templates available.

- NIST Special Publication 800-171r3, CUI-SSP Template (see Exhibit B)
- NIST Special Publication 800-53r5, System Security Plan (SSP) Template (see Exhibit C)
- NIST Special Publication 800-171r3, System Security Plan (SSP) (see Exhibit D)
- SSA PII Loss Reporting Template (see Exhibit E)

Additionally, see the section "SAFEGUARDING FEDERAL TAX INFORMATION REQUIREMENTS" which outlines additional requirements if Federal Tax Information (FTI) is involved.

PHYSICAL SECURITY: Contractor's facilities storing SSA assets and information are required to meet the Interagency Security Committee's (ISC) standard for Federal facilities. This information can be found in the "Facility Security Plan: An Interagency Security Committee Guide," dated February 2015, 1st Edition. SSA reserves the right to inspect contractor facilities to ensure compliance with the ISC guidelines. If facilities are found deficient, the contractor must implement corrective actions within 45 calendar days of notification. Requirements can include, but not be limited to, the physical security countermeasures, such as access control systems, closed circuit television systems, intrusion detection systems, and barriers.

Contractor must pass all External Service Provider Security and Physical Security requirements as specified above before the Government can award this contract. Any bidder who cannot obtain approval for any of these security requirements within 60 calendar days of approval of production plans and physical security inspection will be declared non-responsible.

SECURITY WARNING:

All employees working on this contract must:

- Be familiar with current information on security, privacy, and confidentiality as they relate to the requirements of this contract.
- Obtain pre-screening authorization before using sensitive or critical applications pending a final suitability determination as applicable to the specifications.
- Lock or log off their workstation/terminal prior to leaving it unattended.
- Act in an ethical, informed, and trustworthy manner.
- Protect sensitive electronic records.
- Be alert to threats and vulnerabilities to their systems.
- Be prohibited from having any mobile devices or cameras in sensitive areas that contain confidential materials, including areas where shredding and waste management occurs.

Contractor's managers working on this contract must:

- Monitor use of mainframes, PCs, LANs, and networked facilities to ensure compliance with national and local policies, as well as the Privacy Act statement.
- Ensure that employee screening for sensitive positions within their department has occurred prior to any individual being authorized access to sensitive or critical applications.
- Implement, maintain, and enforce the security standards and procedures as they appear in this contract and as outlined by the contractor.
- Contact the security officer within 24 hours whenever a systems security violation is discovered or suspected.

Applicability: The responsibility to protect PII applies during the entire term of this contract and all option year terms if exercised. All contractors must secure and retain written acknowledgement from their employees stating they understand these policy provisions and their duty to safeguard PII. These policy provisions include, but are not limited to, the following:

- Employees are required to have locking file cabinets or desk drawers for storage of confidential material, if applicable.
- Material is not to be taken from the contractor's facility without express permission from the Government.
- Employees must safeguard and protect all Government records from theft and damage while being transported to and from contractor's facility.

The following list provides examples of situations where PII is not properly safeguarded:

- Leaving an unprotected computer containing Government information in a non-secure space (e.g., leaving the computer unattended in a public place, in an unlocked room, or in an unlocked vehicle).
- Leaving an unattended file containing Government information in a non-secure area (e.g., leaving the file in a break-room or on an employee's desk).
- Storing electronic files containing Government information on a computer or access device (flash drive, CD, etc.) that other people have access to (not password-protected).

This list does not encompass all failures to safeguard PII but is intended to act as an alert to the contractor's employees to situations that must be avoided. Misfeasance occurs when an employee is authorized to access Government information that contains sensitive or personally identifiable information and, due to the employee's failure to exercise due care, the information is lost, stolen, or inadvertently released.

Clause 2352.224-2A Protecting and Reporting the Loss of Personally Identifiable Information (May 2019)

(a) *Definitions.*

The following terms are defined for the purposes of this clause:

"Agency" means the Social Security Administration (SSA).

"Breach" means the loss of control, compromise, unauthorized disclosures, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses personally identifiable information (PII); or (2) an authorized user accesses or potentially accesses personally identifiable information for another than authorized purpose. A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PII for other than an authorized purpose. Often, an occurrence may be first identified as an incident, but later identified as a breach once it is determined that the incident involves PII, as is often the case with a lost or stolen laptop or electronic storage device.

Some common examples of a breach include:

- A laptop or portable storage device storing PII is lost or stolen;
- An email containing PII is inadvertently sent to the wrong person;
- A box of documents with PII is lost or stolen during shipping;
- An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or Federal benefits;
- A user with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual;
- An information technology system that maintains PII is accessed by a malicious actor; or
- PII that should not be widely disseminated is posted inadvertently on a public website.

"Employee(s)" means individual(s) under a direct employee-employer relationship with the contractor, where the contractor has the power or right to control and direct the individual in the material details of how work is to be performed.

"Handling of PII" or "handle(s) PII" means accessing, using, creating, collecting, processing, storing, maintaining, disseminating, disclosing, disposing, or destruction of PII, as defined in this clause.

"Incident" means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

"Personally identifiable information" (PII) means 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. The PII may range from common data elements such as names, addresses, dates of birth, and places of employment, to identity documents, Social Security numbers (SSN) or other government-issued identifiers, precise location information, medical history, and biometric records. Within this clause, "PII" shall specifically mean PII that is made or becomes available to the contractor, including its employees, as a result of performing under this contract.

"Primary agency contact" means the SSA Contracting Officer's Representative (COR) who is the Contracting Officer's Technical Representative (COTR) or, for indefinite delivery contracts with individual orders issued against the contract, e.g., task-order contracts, the order's Task Manager, if one has been assigned. The COR may have one or more designated alternates to act for the COR when the COR is unavailable. If neither the COR nor the designated alternate is available, the alternate shall be considered a responsible agency manager in the office.

"Secure area" or "Secure duty station" means, for the purpose of this clause, either of the following, unless the agency expressly states otherwise on a case-by-case basis: (1) a contractor employee's official place of work that is in the contractor's established business office in a commercial setting, or (2) a location within the agency or other Federal- or State-controlled premises. A person's private home, even if it is used regularly as a "home office" (including that of a contractor management official), shall not be considered a secure area or duty station.

"Suspected breach" means PII that, among other possibilities, has been lost or stolen, or accessed in an unauthorized fashion, but it is not yet confirmed that the PII has been compromised to meet the level of a breach.

"Transport(ing)" or "transported" means the physical taking or carrying of PII from one location to another. For the purpose of this clause, the term does not include shipping by a common or contract carrier (as defined in Federal Acquisition Regulation (FAR) section 47.001), shipping by the U.S. Post Office, or electronic transmission. See "FILE TRANSFER MANAGEMENT SYSTEM (FTMS) REQUIREMENTS" specified herein for information regarding electronic transmission. SSA will review and approve the Material Handling and Inventory Control plan and the Security Control Plan (see "PREAWARD PRODUCTION PLANS, *Materials Handling and Inventory Control Plan"* and *"Security Control Plan*"). The plans shall describe in detail how the contractor will transport PII.

(b) *Responsibility for Safeguarding PII.*

(1) The contractor shall comply with applicable limitations on use, treatment, and safeguarding of PII under the Privacy Act of 1974 (5 U.S.C. § 552a); the Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, et seq.), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); related National Institute of Standards and Technology guidelines; the Paperwork Reduction Act, 44 U.S.C. § 3501-3521; the E-Government Act of 2002, 44 U.S.C. § 3501 note; Office of Management and Budget (OMB) guidance relating to handling of PII, including OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information"; SSA privacy and security policies and procedures relating to handling of PII; and other Federal laws governing handling of PII.

(2) The contractor shall establish, maintain, and follow its own policies and procedures to protect the confidentiality of PII (PII policies and procedures) in accordance with the laws, policies, and requirements referenced in this clause and elsewhere in the contract. The contractor's PII policies and procedures shall include safeguards to protect PII from loss, theft, or inadvertent disclosure and breach procedures.

(3) The contractor shall restrict handling of PII to only those authorized employees who need it in connection with the performance of work under this contract.

(4) Unless authorized by this contract or otherwise in writing by SSA, the contractor shall not publish, disclose, release, or otherwise disseminate PII, internally or externally.

(5) The contractor shall inform its employees who will or may handle PII of their individual responsibility to safeguard it. In addition, the contractor shall educate and train employees as required by FAR 24.301 and enforce employees' compliance with the contractor's PII policies and procedures and other requirements relating to handling of PII in this contract. SSA may require the contractor to provide evidence of the performance of training and the content of the training.

(6) Additional policies, procedures, and requirements involving the handling of PII may be prescribed elsewhere in this contract, including but not limited to information security policies. The contractor shall follow all such policies, procedures, and requirements. If contract performance calls for the contractor handling of PII in a manner not addressed in this clause or elsewhere in the contract that may cause a security question or concern, the contractor shall seek clarification and direction from the agency, prior to commencing the handling of PII in question. The contractor shall also follow the safeguard requirements set forth in "SAFEGUARDING FEDERAL TAX INFORMATION REQUIREMENTS."

(c) *Safeguarding Requirements.*

(1) The contractor is responsible for safeguarding PII at all times. The contractor shall ensure that PII remains under the immediate supervision and control of authorized employees in a manner that will protect the confidentiality and integrity of PII. Examples of proper safeguarding include, but are not limited to: maintaining the confidentiality of each employee's individual password (by not sharing the password with any other individual or entity and not writing it down); verifying the identity of individuals before disclosing information to them; preventing others in the area from viewing PII on one's computer screen; consistently locking or logging off one's workstation when one is away; and ensuring that PII is appropriately returned or, upon receiving the agency's approval, destroyed when no longer needed. The contractor may use its internal policies and practices, non-disclosure agreements, system security requirements or any other means to accomplish its safeguarding responsibilities.

(2) *Transporting PII Outside a Secure Area/Secure Duty Station.*

(i) The contractor shall safeguard equipment, files, or documents containing PII when transporting information from a secure area/secure duty station. The contractor shall ensure that the laptops and other electronic devices/media being used to transport PII are encrypted and password protected. The contractor shall ensure that the encryption and password protection are in accordance with any agency-prescribed standards or policies, which shall be communicated separately from this clause. The contractor shall use reasonable protection measures when transporting PII, e.g., storing files in a locked briefcase, not leaving files and/or equipment in plain view.

(ii) The contractor shall ensure that its PII policies and procedures address transporting PII outside a secure area and emailing PII to and from non-SSA email addresses. The contractor shall provide employees, upon or immediately prior to their commencing work on the contract, with contact information and instructions relating to PII breaches and incidents, based on the contractor's security/PII loss incident policy and procedures. (If the preceding requirement is introduced to the contract under a contract modification, the contractor shall ensure employees are provided this information and instructions within 10 working days of the modification.) The contractor shall periodically remind employees of the foregoing information and instructions per the regular training requirements at (d)(1) below.

(NOTE: Agency-prescribed contact information and instructions for reporting lost or possibly lost PII are discussed in paragraph (d) below.) SSA may require that the contractor present evidence of compliance with these provisions.

(iii) *Tracking PII-containing material (files, documents, etc.).*

(A) Unless the PII is being transported for disposal pursuant to the contract per (c)(3) below, or SSA grants an exception per (c)(2)(iii)(D) below, the contractor shall take appropriate and necessary action to ensure that the PII-containing material, such as file(s) or document(s) being physically transported or transmitted electronically outside the secure area/secure duty station, are tracked through a log. The PII-containing material shall be logged out prior to transport as well as logged back in upon return. The contractor can establish any mechanism for tracking as long as the process, at a minimum, provides for the following information to be logged:

(1) first and last name of the employee taking/returning the material;

(2) the identification of the PII-containing material, such as the name of the file(s) or document(s) containing PII;

(3) the media used to transport the PII (e.g., electronic, such as laptop, portable drive, compact disc/digital versatile disc (CD/DVD), or email—be as specific as possible; paper, such as paper file folders or printouts);

(4) the reason he/she intends to transport the PII-containing material;

(5) the date he/she transported the PII-containing material from the secure area/secure duty station;

(6) the date the PII-containing material is due to be returned to the secure area/duty station. See subparagraph (c)(2)(iii)(B) immediately below.

(7) the approver's name and phone number.

(8) the actual return date of the PII-containing material.

(B) Materials shall be returned or, when authorized by paragraph (c)(3), documented as destroyed, within 90 calendar days of removal from the office or have contractor supervisory approval for being held longer.

(C) The log shall be maintained in a secure manner. Upon request by the agency, the contractor shall provide the information from the log in a format (e.g., electronic or paper) that can be readily accessed by the agency. The contractor shall retain the log in accordance with General Records Schedule 4.2, Information Access and Protection Records, Item 40 (disposition authority DAA-GRS-2016-0002-0004). (See Exhibit F.)

(D) SSA may relieve the contractor of having to comply with these logging requirements for certain transmissions when the contractor is engaged in routine and secure transmission of PII, and SSA determines that there are appropriate security controls in place to track the data through other means.

(3) *Return and/or Disposal of PII.* The contractor shall return and/or dispose of the PII when the PII is no longer required for performance of this contract, e.g., upon contract completion, per agency direction and requirements. The marked statement(s) below apply to this contract:

[x] (i) This contract entails the return of PII.

[x] (ii) This contract entails the disposal of PII. The contractor shall follow the procedures described in "Disposal of Waste Materials" (see "PREAWARD PRODUCTION PLANS, *Disposal of Waste Materials*").

(4) *Emailing PII.* The contractor's corporate or organizational email system is deemed not to be secure. Therefore, the contractor shall put policies and procedures in place to ensure that its employees email PII using only the following procedures in (i) and (ii), below:

(i) *Sending from a SSA email address*. If employees have been given access to the SSA email system, they may use it to send email messages containing PII in the body or in an unencrypted attachment but only to other SSA email addresses (which contain the "name@ssa.gov" format) or to email addresses belonging to a SSA-certified email system. Email directed to any other address(es) may contain PII only if the PII is entirely contained in an encrypted attachment. The contractor shall encrypt PII in accordance with OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016).

(ii) *Sending from a non-SSA email system*. If employees are using the contractor's own or any other non-agency email system (e.g., Yahoo!, Gmail), they may send email messages transmitting PII only if the PII is entirely contained in an encrypted attachment, per OMB Circular A-130; none of the PII may be in the body of the email itself or in an unencrypted attachment. When emailing from such systems, this procedure applies when emailing PII to any email address, including but not limited to, a SSA email system address. Unless specifically noted otherwise, the contractor and its employees are expected to conduct business operations under this contract using the contractor's own email system, i.e., in accordance with the foregoing rules for transmitting PII.

SSA may grant written exceptions to compliance with the email requirements in paragraph (c)(4) above when the contractor's corporate or organizational email system has been deemed by SSA to be secure.

(d) *Procedures for Reporting PII Breach or Incident*. The agency has its own reporting requirements for PII breaches or incidents. The purpose of the following paragraphs is to ensure that the contractor meets the requirements and shares breach or incident information appropriately. The contractor's report of a breach or incident will not, by itself, be interpreted as evidence that the contractor failed to provide adequate safeguards for PII.

(1) *Contractor Responsibility.* In addition to establishing and implementing its own internal procedures referenced in paragraph (b) above, the contractor shall provide regular training (at least annually and when new employees commence work) for contractors on how to identify and report a breach or incident and take reasonable actions to implement agency-prescribed procedures described in paragraph (d)(3) below for reporting PII breaches or incidents. These include training employees handling PII about these procedures, including how to identify and report a PII breach or incident, and otherwise taking appropriate and necessary steps to enforce their compliance in carrying them out. The contractor shall cooperate and exchange information with agency officials, as determined necessary by the agency, in order to report and manage a suspected or confirmed breach or incident effectively. The contractor shall maintain capabilities to determine what agency information was or could have been accessed and by whom, be able to construct a timeline of user activity, determine methods and techniques used to access agency information, and identify the initial attack vector. The contractor shall allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with OMB memorandum M-17-12 and agency guidance and breach procedures to assist with responding to a breach or incident. SSA may require evidence of compliance with this guidance.

(2) *Potential Need for Immediate, Direct Reporting by the Employee.* The agency recognizes that contractor employees will likely make the initial discovery of a PII breach or incident. When an employee becomes aware or suspects that PII has been lost or compromised, he/she is required to follow the contractor's established security/PII breach/incident reporting process (see paragraph (d)(1), above). The contractor's reporting process, along with the agency's (see paragraph (d)(3) below), shall require the contractor, and not necessarily the employee, in such circumstances to notify the agency of the breach or incident. However, the contractor shall inform each employee handling or potentially handling PII that he/she must be prepared to notify outside authorities directly and immediately as described in paragraph (d)(3)(v) below, if, shortly following the breach or incident or discovery of the breach or incident, he/she finds it evident that neither an appropriate contractor nor the agency manager/contact can be reached. The contractor shall emphasize to the employee that timeliness in reporting the incident is critical.

(3) *Procedures*.

(i) When a contractor employee becomes aware of or suspects a PII breach or incident, the contractor, in accordance with its incident reporting process, shall provide immediate (as soon as possible and without unreasonable delay) notification of the breach or incident to the primary agency contact. If the primary agency contact is not readily available, the contractor shall immediately notify the contact's alternate. The contractor shall act to ensure that each employee, prior to commencing work on the contract, has been given information as to who the primary and alternate agency contacts are and how to contact them. In addition, the contractor shall act to ensure that each employee promptly receives any updates on such information, as they are made available. Whenever the employee removes PII from a secure area/secure duty station, he/she shall comply with the contractor's security policies, including having on hand the current contact information for the primary agency contact and at least one alternate.

(ii) The contractor shall provide the primary agency contact or the alternate, as applicable, updates on the status of the reported PII loss or compromise as they become available but shall not delay the initial report.

(iii) The contractor shall provide complete and accurate information about the details of the PII breach or incident to assist the agency contact/alternate, including the following information:

(A) Contact information;

(B) A description of the PII breach or incident (i.e., nature of the breach, scope, number of files or records, type of equipment or media, etc.) including the approximate time and location of the loss;

(C) A description of safeguards used, where applicable (e.g., locked briefcase, redacted personal information, password protection, encryption, etc.);

(D) An identification of agency components (organizational divisions or subdivisions) contacted, involved, or affected;

(E) Whether the contractor or its employee has contacted or been contacted by any external organizations (i.e., other agencies, law enforcement, press, etc.);

(F) Whether the contractor or its employee has filed any other reports (i.e., Federal Protective Service, local police, and agency reports); and

(G) Any other pertinent information.

(iv) The contractor may use the PII Loss Reporting Template (Exhibit E) to gather and organize information quickly about the incident. The contractor shall ensure that each employee with access to PII under the contract, prior to accessing the PII, has a copy of the worksheet with its instructions, and particularly when transporting PII from a secure duty station.

(v) There may be rare instances (e.g., outside of business hours) when the contractor is unable to reach either the primary agency contact or the alternate immediately. In such a situation, the contractor shall immediately call the agency's Enterprise Customer Service Desk (ECSD) toll-free at 1-877-697-4889 to file the initial report directly, providing the information in (d)(3)(iii) above and as requested by the ECSD. Overall, during this time, the contractor shall cooperate as necessary with the ECSD or any of the other external organizations described in (d)(3)(iii) above.

(vi) If the contractor makes a direct report to the ECSD, the contractor shall document the call with the Enterprise Customer Support (ECS) Ticket number, which the ECSD will assign. The contractor shall provide the ECS Ticket number to the primary agency contact, or, if unavailable, his/her alternate.

(vii) Subparagraphs (v) through (vi) apply to all contractor employees. The contractor shall ensure its internal procedures and PII breach/incident training make clear to employees these responsibilities. Reports to the ECSD should not be delayed because an employee could not reach the contractor's management.

(viii) The contractor and its employee(s) shall limit disclosures about PII involved in a breach or incident to only those SSA and contractor employee(s) with a need for the information in order to respond to and take action to prevent, minimize, or remedy the breach or incident. The contractor may disclose breach or incident information to Federal, state, or local law enforcement agencies and other third parties with a need for the information; however, information about the specific PII involved may only be disclosed to such authorities and third parties as Federal law permits. The contractor shall not, without SSA approval, publicly disclose information about PII involved in a breach or incident or SSA's involvement in a breach or incident. The contractor shall not, without SSA approval, notify individuals affected by the PII breach or incident. The contractor's PII breach and incident reporting process shall ensure that disclosures are made consistent with these requirements. As used in this paragraph, the term PII references only PII covered by this clause.

(e) *Additional Contractor Responsibilities When There Is a Suspected or Confirmed Breach.*

(1) The contractor shall have a formal security/PII breach or incident reporting process in place that outlines appropriate roles and responsibilities, as well as the steps that must be taken, in the event of a security/PII breach or incident. The plan shall designate who within the contractor's organization has responsibility for reporting the PII breach or incident to the agency.

(2) In the event of a PII breach or incident, the contractor shall take immediate steps to address consequential security issues that have been identified, including steps to minimize further security risks to those individuals whose personal information was lost, compromised, or potentially compromised.

(3) The contractor shall confer with SSA personnel in reviewing the actions the contractor has taken and plans to take in dealing with the breach or incident. Additionally, the contractor shall provide any documentation requested by SSA.

(4) The contractor shall bear the cost for any data breach or incident: (1) occurring outside of SSA-controlled facilities, systems, or environments when the affected PII was in the possession or control of the contractor or its employees, agents, or representatives; or (2) resulting from the contractor or its

employees, agents, or representatives' failure to properly safeguard PII or facilities, systems, or other environments containing PII in accordance with this contract's requirements. In addition, as SSA requires, the contractor shall be responsible for or shall assist SSA in taking preventative and remedial actions that SSA determines are necessary to address such a breach or incident.

Preventative and remedial actions may include notification to individuals potentially affected by the breach and other countermeasures to mitigate the risk of harm or to protect PII (e.g., operating call centers and providing resources for potentially affected individuals). SSA will notify the contractor when SSA determines that preventative or remedial action(s) are necessary and instruct the contractor on whether the action(s) will be effectuated by the contractor or SSA. SSA may choose to effectuate the action(s) at the agency's discretion. The contractor shall be responsible for the cost of all preventative or remedial action(s), including those actions effectuated by SSA, resulting from the breaches and incidents covered by this paragraph. Note: Nothing in this paragraph affects the contractor's obligations in paragraph (e)(2) above to take immediate steps to address identified security issues.

(f) *Subcontractor(s).*

(1) The contractor shall include this clause in all resulting subcontracts whenever there is any indication that the subcontractor(s) and their employees, or successor subcontractor(s) and their employees, will or may handle PII. When this clause is included in a subcontract, all references to "contractor" in paragraphs (a) through (e) and (h) shall be read to apply to the subcontractor(s).

(2) The contractor shall take appropriate and necessary action to ensure its subcontractor(s) and their employees, or any successor subcontractor(s) and their employees, comply with this clause.

(3) *Notification of Subcontractor Handling of PII*. If the contractor engages a subcontractor under this contract whose employee(s) will actually or potentially handle PII, the contractor shall do the following:

(i) Notify the SSA COR-COTR and the Contracting Officer of this arrangement in advance of providing access to PII, providing the subcontractor name(s) and address(es) and, upon request, a description of the nature of the PII to which the employee(s) will actually or potentially be given/have access (e.g., phone numbers, SSN); and

(ii) Provide the agency's COR-COTR the names of the subcontractor employee(s) who will actually or potentially be assigned and/or have access to the PII. The contractor may satisfy this requirement when submitting the name(s) of the subcontractor employee(s) to the agency's COR-COTR for the requisite security background check described in paragraph (g) below.

(g) *Security and Suitability Requirements Clause.* For each contractor employee handling PII, the contractor shall fulfill the requirements of the Security and Suitability Requirements Clause, found elsewhere in this contract, to ensure that any such individual has the appropriate background checks.

(h) The contractor shall permit the agency to conduct security reviews and inspections to ensure that the contractor maintains adequate safeguards and security measures for PII in accordance with the terms of this contract. At SSA's request, the contractor shall grant SSA, and its auditors, access to all systems, facilities, equipment, locations, and other environments that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII for such reviews and inspections. The contractor is not required to provide SSA access to parts of those systems, facilities, equipment, locations, and other environments that are not impacted by such reviews and inspections.

SAFEGUARDING FEDERAL TAX INFORMATION REQUIREMENTS:

The contractor and contractor's officers and employees must be in compliance with all requirements of IRS Publication 1075 – "Tax Information Security Guidelines for Federal, State and Local Agencies" (Revised November 2021) as applicable to this contract, with particular attention to the following information –

NOTE: The below information, in its entirety, can be found in IRS Publication 1075; however, some edits have been made specific to SSA and this contract. Any edits made do not change the requirements of IRS Publication 1075 or relieve the contractor or contractor's officers and employees of being in compliance with IRS Publication 1075 and the requirements of this contract. IRS Publication 1075 can be accessed at: P 1075 (Rev. 11-2016) (irs.gov).

"Federal Tax Information" (FTI) includes return or return information received directly from the IRS or obtained through an authorized, secondary source, including SSA.

"Return" means any tax or information return, estimated tax declaration or refund claim required by or permitted under the IRC and filed with the IRS by, on behalf of, or with respect to any person or entity.

"Return Information" is any information collected or generated by the IRS regarding any person's liability or possible liability under the IRC. It includes but is not limited to:

- Information that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRC for any tax, penalty, interest, fine, forfeiture, or other imposition or offense
- Information extracted from a return, including names of dependents or the location of business
- The taxpayer's name, address, and identification number
- Information collected by the IRS about any person's tax affairs, even if identifiers, such as name, address, and identification number, are deleted
- Status of whether a return was filed, under examination, or subject to other investigation or processing, including collection activities
- Information contained on transcripts of accounts

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

(1) All work will be performed under the supervision of the contractor.

(2) The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to SSA and, upon request, to the IRS.

(3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

(4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

(5) The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time

the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to SSA. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide SSA with a statement containing the date of destruction, description of material destroyed, and the destruction method.

(7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

(8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS and SSA. (NOTE: Any subcontracting must be in accordance with the subcontracting requirements of this contract).

(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

(10) To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties, and responsibilities that SSA under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties, and responsibilities which the contractor assumes toward SSA under this contract.

(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to SSA under this contract.

(12) For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

(13) SSA will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five (5) years, or both, together with the costs of prosecution.

(2) Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as one (1) year, or both, together with the costs of prosecution.

(3) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection, or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access, inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A, and 7431 and set forth at 26 CFR 301.6103(n)-1.

(4) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who, knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(5) Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands SSA's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of SSA's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in SSA's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on SSA's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10.) For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and SSA, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process, or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

NOTE: The foregoing inspection rights are in addition to such rights identified elsewhere in this contract. Inspection rights identified elsewhere in this contract are not diminished or modified by these rights.

2352.204-1 – Security and Suitability Requirements (Sept 2023)

NOTE: For the purposes of this contract, the Contracting Officer's Representative (COR) or Contracting Officer's Technical Representative (COTR) is the SSA representative/Program Lead. Additionally, the terms "business days," "working days," and "workdays" are used interchangeably throughout this contract.

(a) Acronyms and Definitions – As used in this clause –

"Applicant" means an individual seeking to work on or for an SSA contract or grant.

"Access to a facility, site, system, or information" means physical access to any Social Security Administration (SSA) facility or site, logical access to any SSA information system, or access to programmatic or sensitive information.

"CO" means contracting officer.

"Contractor" means any entity having a relationship with SSA because of this contract. This term includes, but is not limited to, corporations, limited liability partnerships, and sole proprietorships.

"Contractor personnel" means employees of the contractor, employees of the subcontractor, any consultant retained by the contractor or subcontractor, any volunteer or intern of the contractor or subcontractor, and if the contractor or subcontractor is a sole proprietorship, it refers to the sole proprietorship.

"COR" means contracting officer's representative.

"CPOC" means company point of contact as specified by the contract.

"CSPS" means Center for Suitability and Personnel Security.

"eAPP" means electronic application. "eAPP" contains the investigative Standard Forms (SF) federal applicants use to input information required to process their personnel background investigation. eAPP replaced eQIP as the system for initiating investigations.

"NBIS" means National Background Investigation Services.

"PIV" means Personal Identity Verification.

"Subcontractor" means any entity having a relationship with SSA's contractor because of this contract. This term includes, but is not limited to, corporations, limited liability partnerships, and sole proprietorships.

(b) Purpose

This clause provides SSA's policies and procedures concerning the conduct of background investigations (i.e., suitability determinations) of contractor personnel. A background investigation is required any time contractor personnel requires any type of access to a facility, site, system, or information, whether or not a PIV credential is required. Contractor personnel may be subject to periodic reinvestigation per SSA policy. The purpose of these investigations is to determine the suitability of contractor personnel needing access to a SSA facility, site, system, or information. If applicable, the clause also describes the process to obtain a PIV credential.

PIV Credentials

(1) A PIV credential is required for contractor personnel requiring access to a SSA information system or routine, unescorted access to a SSA facility or site for a period of six months or more. (See paragraph (k) for more information.)

(2) A PIV credential is not required for:

(i) Contractor personnel requiring escorted access to a SSA facility or site for less than six months; or

(ii) Contractor personnel requiring infrequent escorted access to a SSA facility or site, even if the access may be longer than six months (e.g., contractor personnel who provide infrequent facilities or equipment maintenance or repair, or who conduct onsite shredding, etc.).

(c) Authorities

(1) Homeland Security Presidential Directive 12 (http://www.dhs.gov/homeland-security-presidential-directive-12).

(2) Office of Management and Budget Memorandum M-05-24 (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf).

(3) The Crime Control Act of 1990, Public Law 101-647, subtitle E, as amended by Public Law 102-190 (for childcare center security requirements) (http://www.gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap132-subchapV-sec13041.pdf).

(4) Executive Orders 13764 and 12968 (https://www.hsdl.org/?abstract&did=798174 and https://www.gpo.gov/fdsys/pkg/FR-1995-08-07/pdf/95-19654.pdf)

(5) Title 5, Code of Federal Regulations (CFR), Parts 731, 736, and 1400 (for positions assigned a "National Security" designation) (http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title05/5cfr731_main_02.tpl, http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title05/5cfr736_main_02.tpl, and http://www.ecfr.gov/cgi-bin/text-idx?SID=ea8d9b7f129b58c4b512ea9d68a44761&mc=true&node=pt5.3.1400&rgn=div5%23se5.3.1400_1201)

(6) Contractors must comply with the Fair Chance to Compete for Jobs Act of 2019 (National Defense Authorization Act for Fiscal Year 2020) and the respective Federal regulations (5 CFR Parts 302, 317, 319, 330, 731, 754, and 920). In accordance with the Fair Chance Act, the contractor may not verbally, or through written form, request the disclosure of criminal history record information regarding an applicant for a position related to work under such contract before the contractor extends a conditional offer to the applicant.

(d) Suitability Process

The background investigation and adjudication processes are compliant with 5 CFR 731 or equivalent.

SSA is required to submit fingerprints to the Federal Bureau of Investigation (FBI) as part of the Federal personnel background investigation process. This requirement is in accordance with Homeland Security Presidential Directive-12 (HSPD-12) and is mandatory for everyone within the SSA workforce, including contractor personnel.

The FBI maintains fingerprints and uses these fingerprint submissions to conduct ongoing post-appointment arrest checks. Consistent with Federal suitability and personnel security regulations and directives, any post-appointment arrest notifications will be sent to CSPS for suitability review.

Contractors must notify their applicants to work on SSA contracts to carefully review and understand the FBI Privacy Act Statement and the Noncriminal Justice Applicant's Privacy Rights Statement, which can be found through the links below. These documents contain vital information about individual's rights and how their information will be handled.

- Privacy Act Statement — FBI
- Noncriminal Justice Applicant's Privacy Rights

Any applicant requiring access to a SSA facility, site, information, or system must complete and submit, through the COR, the documents listed in (1) at least 30 business days prior to the date contractor personnel are to begin work. The suitability process cannot begin until the contractor submits, and SSA receives, accurate and complete documents.

(1) Suitability Document Submission

a. Immediately upon award, the CPOC must provide to the COR for all applicants requesting a suitability determination:

(i) An Applicant Listing including the names of all applicants requesting suitability;
(ii) Completed Optional Form (OF) 306, Declaration for Federal Employment (see Exhibit G);
(iii) Proof of citizenship and/or work authorization documents for non-U.S. born applicants, if applicable.

b. The Applicant Listing must include the contractor's name, the contract number, the CPOC's name, the CPOC's contact information, the COR's name, the COR's contact information, Social Security Number (SSN), First Name, Full Middle Name, Last Name, Suffix, Email Address, Date of Birth (MM/DD/YYYY), Birth City, Birth County, Country (if not USA), Birth State/Province for all applicants requesting suitability. All spelling of names, email addresses, places, and numbers must be accurate, consistent, and legible.

The required suitability forms and a sample of properly completed forms are available on SSA's Office of Acquisition and Grants (OAG) website ("Information About Acquisitions" tab, "Security Information" section [https://www.ssa.gov/oag/acq/ASC_2352_204-1_Security_and_Suit_Reqrmts_Post_10012017/Links%20for%20Agency%20Specific%20Clause%202352_204-1%20Post%2010012017.htm]).

(2) eApp Form and Fingerprint Submission

a. Once SSA receives all completed documents, listed in (1), CSPS will initiate the suitability screening process using the Applicant Listing. CSPS will email the specific suitability instructions to the CPOC and COR for applicants to electronically complete the background investigation form (Standard Form (SF) 85, Questionnaire for Non-Sensitive Positions or SF 85P, Questionnaire for Public Trust Positions – see Exhibit H). Applicants will receive two separate account creation emails from donotreply@nbis.mil. One email contains the User ID and link with instructions. The other email has the applicant's temporary password.

b. Applicants should complete their investigative forms as soon as possible but no later than seven business days from receipt of the account creation emails. After form submission, applicants can download copies of their form and relevant documents. Please note, reviewing the form prior to submission can only be done in eAPP. The SF does not become available for download until it has been submitted in eAPP.

c. Information about the eApp process is available on the National Background Investigative Services (NBIS) website.

d. CSPS will also email instructions to the CPOC and COR for applicants to obtain electronic fingerprinting services. Applicants must schedule a fingerprint appointment and submit fingerprints as soon as possible. Please note, fingerprinting should not be completed until after the eAPP has been submitted.

If applicants cannot report to the designated fingerprint locations (in the notification email), CSPS will accept completed Field Division (FD) 258 fingerprint cards (see Exhibit I). The COR can provide the FD 258, if required. Applicants must complete all fields on the FD 258. Incomplete fields may delay suitability processing.

If applicants need to mail completed FD 258 fingerprint cards, the applicants are to send them, via certified mail, along with a completed Contractor Personnel Suitability Cover Sheet-Fingerprint Cards (found on the OAG website) to:

Social Security Administration
Center for Suitability and Personnel Security
Attn: Contractor Security Team
6401 Security Boulevard
2246 Annex Building
Baltimore, MD 21235

(3) Status Check

If applicants have completed each of the steps in their entirety and do not receive a suitability determination within 15 business days of their last submission, call 1-844-874-9940 to determine suitability status.

(e) Suitability Determination

(1) CSPS uses an FBI fingerprint check as part of the basis for making a preliminary suitability determination. This determination is final unless information obtained during the remainder of the full background investigation, conducted by SSA's Investigative Service Provider, is such that SSA would find the contractor personnel unsuitable to continue performing under this contract. CSPS will notify the CPOC and the COR of any unsuitable determinations.

(2) SSA will not allow contractor personnel access to a facility, site, information, or system until CSPS issues a favorable preliminary suitability determination. A prescreen suitability determination letter issued by CSPS is valid only for performance on the contract specified in the letter.

(3) If an applicant previously received a suitability determination from SSA while employed by another contractor and is to perform work under this SSA contract for a different contractor, the CPOC must submit a fully completed, legible Contractor Personnel Rollover Request Form (see Exhibit J) to the COR of the new contract. CSPS will notify the CPOC and the COR of suitability to work on this contract. The Contractor Personnel Rollover Request Form is on OAG's website.

(f) Contractor Personnel Previously Cleared by SSA or Another Federal Agency

If an applicant previously received a suitability determination from SSA or another Federal agency, all documentation will be reviewed to determine reciprocity. If reciprocity applies, there will be no eAPP initiated. However, fingerprints will be required for all cases including reciprocity.

(g) CSPS will then provide a letter to the CPOC and the COR indicating the applicant is suitable to begin work on the contract. A contractor is not entitled to an equitable adjustment of the contract because of an unfavorable suitability determination(s). Additionally, if SSA determines that the number or percentage of unfavorable determinations make successful contract performance unlikely, SSA may terminate the contract for cause or default.

(h) Unsuitable Determinations

(1) The contractor must notify the contractor personnel of any unsuitable determinations as soon as possible after receipt of such a determination.

(2) The contractor must submit requests for clarification for unsuitable determinations in writing within 30 calendar days of the date of the unsuitable determination to the email mailbox or address listed below. Contractor personnel must file their own requests; contractor may not file requests on behalf of contractor personnel.

dchr.ope.suitclarify@ssa.gov

OR

Social Security Administration
Center for Suitability and Personnel Security
Attn: Contractor Security Team
6401 Security Boulevard
2246 Annex Building
Baltimore, MD 21235

(3) There is no appeals process for contractor unsuitable determinations.

(i) Contractor Notification to Government

The contractor shall notify the COR and CSPS within one business day if any contractor personnel is arrested or charged with a crime during the term of this contract, or if there is any other change in the status of contractor personnel (e.g., leaves the company, no longer works under the contract, the alien status changes, etc.) that could affect their suitability determination. The contractor must provide in the notification as much detail as possible, including, but not limited to: name(s) of contractor personnel whose status has changed, contract number, the type of charge(s), if applicable, date of arrest, the court date, jurisdiction, and, if available, the disposition of the charge(s).

(j) Obtaining a Credential

(1) This section applies only if contractor personnel will have access to a SSA information system or routine or unescorted access to a SSA facility or site for a period of six months or more as described in paragraph (b)(1).

(2) Once the contractor personnel receive notification of an acceptable preliminary suitability determination, but prior to beginning work under the contract, the contractor personnel must appear at the respective SSA facility to begin the credentialing process. The contractor must contact the COR to arrange for credentialing. Once the COR makes the appointment, the COR must contact the contractor to inform the contractor of the credentialing appointment(s). The COR will also arrange for the contractor personnel to be escorted (by either the COR or a COR's representative) to the appropriate credentialing office at the time of this appointment. The contractor personnel must present the preliminary suitability determination letter and two forms of identification at this meeting. At least one of the forms of identification must be a Government-issued photo identification (ID) (for acceptable forms of ID, see List of Acceptable Documents on OAG's website). A signed and dated SSA-222 is also a required document(see OAG's website). For SSA Headquarters access, a completed Form SSA-4395, Application for Access to SSA Facilities, signed by the contractor personnel and the COR is also required. The COR will provide the SSA-4395 Form to the contractor personnel when applicable.

(3) Credentialing appointments last approximately 15 minutes. Depending on a contractor's scheduling needs and availabilities, contractor personnel may be scheduled for credentialing all in one day (this process may take a few hours to complete, depending on the number of contractor personnel that need to be credentialed) or they may come in at separate times convenient to the contractor personnel's and the COR's schedules.

(4) Contacts

a. SSA Headquarters' Parking and Credentialing Office representatives can be reached at Parking.and.Credentialing@ssa.gov or 410-965-5910.

b. Contact information for other SSA facilities is available on OAG's website.

(k) Contractor Return of PIV Credential

The contractor must account for and ensure that all forms of Government-provided identification (PIV credential) issued to contractor personnel under this contract are returned to SSA's Headquarters' Parking and Credentialing Office or respective SSA facility, as appropriate, as soon as any of the following occur: when no longer needed for contract performance; upon completion of any contractor personnel employment; or upon contract completion or termination.

(l) Government Control

The Government has full control over and may grant, deny, or withhold access to a facility, site, system, or information and may remove contractor personnel, or require the contractor to remove contractor personnel from performing under the contract for reasons related to conduct even after contractor personnel are found suitable to work on the contract (see paragraph (m) below).

(m) Removal From Duty

The CO, in coordination with the COR and CSPS, may remove a contractor, or request the contractor immediately remove any contractor personnel from working under the contract based on conduct that occurs after a favorable suitability determination. This includes temporarily removing contractor personnel arrested for a violation of law pending the outcome of any judicial proceedings. The contractor must comply with these requests to remove any contractor personnel. The Government's determination may be made based on, but not limited to, these incidents involving the misconduct or delinquency:

(1) Violation of the Rules and Regulations Governing Public Buildings and Grounds, 41 CFR 101-20.3. This includes any local credentialing requirements.

(2) Neglect of duty, including sleeping while on duty; unreasonable delays or failure to carry out assigned tasks; conducting personal affairs while on duty; and refusing to cooperate in upholding the integrity of SSA's security program.

(3) Falsification or unlawful concealment, removal, mutilation, or destruction of any official documents, records, or Government property or concealment of material facts by willful omissions from official documents or records.

(4) Disorderly conduct, use of abusive or offensive language, quarreling, intimidation by words or actions, or fighting. Also, participating in disruptive activities that interfere with the normal and efficient operations of the Government.

(5) Theft, vandalism, or any other criminal actions.

(6) Selling, consuming, possessing, or being under the influence of intoxicants, drugs, or substances that produce similar effects.

(7) Improper use of official authority or credentials.

(8) Unauthorized use of communications equipment or Government property.

(9) Misuse of weapon(s) or tools used in the performance of the contract.

(10) Unauthorized access to areas not required for the performance of the contract.

(11) Unauthorized access to SSA's employees' personal property.

(12) Violation of security procedures or regulations.

(13) Prior contractor personnel unsuitability determination by SSA or another Federal agency.

(14) Unauthorized access to, or disclosure of, agency programmatic or sensitive information, or Internal Revenue Service Tax Return information.

(15) Failure to ensure the confidentiality of or failure to protect from disclosure, agency information entrusted to them. Certain provisions of these statutes and regulations apply to Federal employees, and apply equally to contractor personnel: The Privacy Act of 1974, The Tax Reform Act of 1976 and the Taxpayer Browsing Protection Act of 1997, SSA regulation 1, The Computer Fraud and Abuse Act of 1986, and Section 1106 of the Social Security Act.

(16) Being under investigation by an appropriate authority for violating any of the above.

(n) The contractor is required to include the substance of this clause in any subcontract requiring the subcontractor to access a SSA facility, site, system, or information. However, the contractor must obtain, review, and submit to SSA all of the completed and required forms (see paragraphs (d) and (e)) from the subcontractor. SSA will not accept completed forms from anyone other than the contractor.

Clause 2352.204-2 Federal Information Security Modernization Act (FISMA) and Agency Privacy Management (MAY 2021)

(a) Definitions

Terms defined for this clause:

"Agency" means the Social Security Administration (SSA).

"COR-COTR" means Contracting Officer's Representative-Contracting Officer's Technical Representative.

"Electronic Personnel Enrollment and Credentialing System (EPECS)" means the system supporting the Homeland Security Presidential Directive-12 credentialing process at SSA.

"OAG" means the Office of Acquisition and Grants at SSA.

"PIV Credential" means personal identity verification credentials required for contractor personnel requiring unescorted access to a SSA facility or access to SSA information systems.

(b) Agency Responsibility Related to FISMA Training Requirements

(1) The Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, et seq.), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283) (collectively, "FISMA"), and the Office of Management and Budget Circular No. A-130 (published July 28, 2016) require all agency contractor and subcontractor personnel working under agency contracts who will have access to any kind of SSA information, receive periodic training in information technology (IT) security awareness and accepted IT security practice. This includes training for contractor personnel who do not have access to electronic information systems. The training level and content is tailored to the contractors' assigned roles and responsibilities and the risk and magnitude of harm related to the required activities.

(2) SSA requires contractor personnel to read and sign the Security Awareness Contractor Personnel Security Certification (CPSC) form, SSA-222. The SSA-222 is on OAG's internet site (see paragraph (c)(3)(i) below) or contractors can ask the COR-COTR for a copy. This training does not preclude any additional role-based information security or privacy training specified elsewhere in this contract.

(c) Contractor Responsibilities Related to FISMA Training Requirements

(1) Contractor Personnel Requiring a SSA-issued PIV Credential and Access to SSA's Network

(i) Following contract award, the agency mandates contractor personnel requiring a PIV credential and access to SSA's network to take security awareness training by reading and electronically signing the CPSC form, SSA-222, during the PIV credentialing process. This requirement also applies to contractor personnel requiring a PIV credential and access to SSA's network subsequently added to the contract. If contractor personnel receive a PIV credential, contractors are not required to send an email per paragraph (c)(3)(iii).

(ii) For each successive year of the contract, contractor personnel shall take annual security awareness training via a video on demand on a SSA-managed website. Contractor personnel with a valid SSA email address will receive an email to take this training at the appropriate time. Additionally, contractor personnel must electronically attest to the CPSC form, SSA-222, within EPECS. The COR-COTR will email this invitation to contractor personnel initiating this action.

(2) Contractor Personnel Requiring a SSA-issued PIV Credential but Not Access to SSA's Network:

(i) Following contract award, the agency mandates contractor personnel requiring a PIV credential to take security awareness training by reading and electronically signing the CPSC form, SSA-222, during the PIV credentialing process. This requirement also applies to contractor personnel subsequently added to the contract and requiring a PIV credential. For contractor personnel receiving a PIV credential, contractors are not required to send an email per paragraph (c)(3)(iii) for the first year of the contract.

(ii) For each successive year of the contract, the contractor shall repeat the processes described in paragraphs (c)(3)(i) through (iii), below, on an annual basis. The contractor must submit the information in paragraph (c)(3)(iii), below, within 45 calendar days of the date the option was renewed, or the anniversary of the contract award date, whichever comes first.

(3) Contractor Personnel Not Requiring a SSA-issued PIV Credential and No Access to SSA's Network:

(i) Following contract award, the contractor shall ensure that all contractor personnel performing under this contract take the security awareness training by reading and signing the CPSC form,

SSA-222. This requirement also applies to contractor personnel subsequently added to the contract. A copy of this form is on OAG's Internet website (SSA-222) (See Exhibit K.)

(ii) The contractor must receive signed copies of the form from each contractor personnel working under the contract within 30 calendar days following contract award, or within 30 calendar days after a contractor personnel begins working under the contract, whichever comes first.

(iii) The contractor shall send an email to the COR-COTR, within 45 calendar days following contract award. Similarly, the contractor shall send such email notification 45 calendar days of when new contractor personnel are added to perform work under the contract. The contractor will attach each signed form, completed per paragraph (c)(3)(ii), above, to the email along with a list of the names (first, middle initial, and last) of the contractor personnel who signed the form and the contract number they are working under.

(iv) For each successive year of the contract, the contractor shall repeat the processes described in paragraphs (c)(3)(i)-(iii), above, on an annual basis. The contractor must submit the information in paragraph (c)(3)(iii), above, within 45 calendar days of the date the option was renewed, or the anniversary of the contract award date, whichever comes first.

(4) The contractor shall retain copies of signed CPSC forms, SSA-222, mentioned in paragraphs (c) (1), (c)(2), and (3) above for potential future SSA audits for a period of three years after final payment (per FAR, Section 4.703).

(d) Applicability of this Clause to Subcontractor Personnel. The contractor is required to include a clause substantially the same as this in all subcontracts awarded under the prime contract. This clause shall require the subcontractors to follow the instructions in paragraph (c) of this clause. For subcontractor personnel following paragraphs (c)(2) and (3), the subcontractor shall submit the signed forms to the contractor and the contractor will be responsible for submitting this information to SSA per paragraph (c)(3)(iii). The subcontractor shall be responsible for maintaining its signed forms as detailed in paragraph (c)(4).

Email Procedures

For the contractor's convenience, SSA has included the following instructions to send emails with sensitive documentation or messages containing personally identifiable information (e.g., SSNs, etc.) securely to a SSA email address. Contractor is to consult their local information technology staff for assistance. If the contractor utilizes an alternate secure method of transmission, it is recommended that the contractor contact the recipient to confirm receipt.

To Encrypt a File using WinZip

i. Save the file to contractor's hard drive.
ii. Open Windows Explorer and locate the file.
iii. Right click on the file.
iv. Select "WinZip."
v. Select "Add to Zip File."
vi. An Add box pops up. Near the bottom of the box is an "Options" area.
vii. Click the "Encrypt added files" checkbox.
viii. Click the "Add" button.
ix. Check the "Hide Password" checkbox if not already checked.
    a. Enter a string of characters as a password composed of letters, numbers, and special characters (minimum 8 characters – maximum 64 characters).
    b. Select the 256-Bit AES encryption radio button.
    c. Click "OK."
x. The file has been encrypted successfully, and the new Zip file can now be attached to an email.

Providing the Recipient with the Password

Send the password to the intended recipient in a separate email message prior to sending the encrypted file or after sending the encrypted file. Do not send the password in the same email message to which the encrypted file is attached.

If possible, it is recommended to provide the password to the COR-COTR by telephone or establish a predetermined password between the contractor and the COR-COTR.

The COR-COTR should also submit the password in a separate email from the documentation when submitting to ^DCHR OPE Suitability. Due to the large volume of submissions, the COR-COTR must always provide the password to ^DCHR OPE Suitability in a separate email, even if it is a pre-established password for a contract.

Sending an encrypted Zip File via email

1. Compose a new message.
2. Attach the Zip File.
3. Send message.

PREAWARD SURVEY: In order to determine the responsibility of the prime contractor or any subcontractor, the Government reserves the right to conduct an on-site preaward survey at the contractor's/subcontractor's facility or to require other evidence of technical, production, managerial, financial, and similar abilities to perform, prior to the award of a contract.

As part of the financial determination, the contractor in line for award may be required to provide one or more of the following financial documents:

1) Most recent profit and loss statement
2) Most recent balance sheet
3) Statement of cash flows
4) Current official bank statement
5) Current lines of credit (with amounts available)
6) Letter of commitment from paper supplier(s)
7) Letter of commitment from any subcontractor

The documents will be reviewed to validate that adequate financial resources are available to perform the contract requirements. Documents submitted will be kept confidential and used only for the determination of responsibility by the Government.

Failure to provide the requested information in the time specified by the Government may result in the Contracting Officer not having adequate information to reach an affirmative determination of responsibility.

Additionally, the preaward survey will include a review of all subcontractors involved, along with their specific functions; and the contractor's/subcontractor's backup facility, quality control/recovery program, computer system, mail, material handling/inventory control, personnel, production, security control, production area, and disposal of waste materials plans as required by this specification.

If award is predicated on the purchase of production and/or systems equipment, the contractor must provide purchase order(s) with delivery date(s) of equipment to arrive, be installed, and be fully functional at least 120 calendar days prior to the start of live production on September 1, 2027.

If the Government, during the preaward survey, concludes that the contractor does not or cannot meet all of the requirements as described in this contract, the contractor will be declared non-responsible.

PREAWARD PRODUCTION PLANS: As part of the preaward survey, the contractor shall present, in writing, to the Contracting Officer within five (5) workdays of being notified to do so by the Contracting Officer or his/her representative, detailed plans for each of the following activities. The workday after notification to submit will be the first day of the schedule. If the Government requests additional information after review of the production plans, the contractor must submit updated plans within two (2) workdays of request.

Additionally, the contractor must submit a Security Authorization Package (SAP) and a Cybersecurity Supply Chain Assessment (CSCRA) Questionnaire (see Exhibit L), as required, within 10 workdays of request. The workday after notification to submit will be the first day of the schedule. If the Government requests additional information after review of the SAP and/or CSCRA Questionnaire, the contractor must submit the additional information within three (3) workdays of request.

NOTE: The schedule for the preaward production plans, SAP, and CSCRA Questionnaire starts the same workday.

After review of the updated plans, SAP, and/or CSCRA Questionnaire, it is at the Contracting Officer's discretion to allow additional revisions.

The Preaward Production Plans must be formatted so that each plan, as specified below, is its own section, and all information required for that plan is specified in that section. At contractor's option, each plan can be a separate document or one document with each plan separately identified.

PLEASE NOTE: The notices produced on this contract must not be produced at multiple facilities, and therefore, cannot be transferred interchangeably between multiple plant locations. Any reference in this contract to multiple locations/facilities refers to the primary location and the backup facility only.

Option Years: For each option year that may be exercised, the contractor will be required to review their plans and re-submit in writing the below plans detailing any changes and/or revisions that may have occurred. The revised plans are subject to Government approval and must be submitted to the Contracting Officer or his/her representative within five (5) workdays of notification of the option year being exercised.

NOTE: If there are no changes/revisions, the contractor will be required to submit to the Contracting Officer or his/her representative a statement confirming that the current plans are still in effect.

These proposed plans are subject to review and approval by the Government, and award will not be made prior to approval of same. The Government reserves the right to waive some or all of these plans.

***Information Sheet* –** If the contractor is currently producing on other GPO contracts, they must submit an information sheet specifying how the workload(s) on this contract will fit into the pre-existing Government production without hampering the production/delivery schedules for all the contracts.

NOTE: This is a requirement of this program due to the legislated nature of certain GPO contracts.

At a minimum, the information sheet must include a list of the contracts currently held and the production/delivery schedules for each of those contracts. The sheet must also specify which of those contracts would run concurrently with the projected schedule for this contract.

***Backup Facility* -** The failure to deliver these notices in a timely manner would have an impact on the daily operations of SSA. Therefore, if for any reason(s) (act of God, labor disagreements, national emergencies, pandemics, etc.), the contractor is unable to perform at said location for a period longer than 24 hours, the contractor must have a backup facility with the capability of producing the notices. The contractor must operate the backup facility.

Plans for their contingency production must be prepared and submitted to the Contracting Officer as part of the preaward survey. These plans must include the location of the facility to be used, equipment available at the facility, security plans at the facility, and a timetable for the start of production at that facility.

Part of the plans must also include the transportation of Government materials from one facility to another. The contractor must produce items from a test file at the new facility for verification of software prior to producing notices at this facility. SSA also has the option to install a connection into the contractor's backup facility.

NOTE: All terms and conditions of this contract will also apply to the backup facility**.** Due to the time-sensitive nature of the notices produced on this contract, the contractor must maintain the original schedule set forth in this contract.

Quality Control Plan – The contractor must provide and maintain, within their organization, an independent quality assurance team of sufficient size and expertise. The team must monitor the operations performed and inspect the products of each operation to a degree and extent that will ensure the Government's quality assurance, inspection, and acceptance provisions specified herein are met. The contractor must perform, or have performed, the process controls, inspections, and tests required to substantiate that the products provided under this contract conform to the specifications and contract requirements. The contractor must describe in detail their quality control/quality assurance and recovery plans describing how, when, and by whom the plans will be performed.

The quality control plan must also include examples and a detailed description of all quality control samples and their corresponding inspection reports or logs the contractor will keep to document the quality control inspections performed on each run. Furthermore, the plan must include the names of all quality assurance officials and describe their duties in relationship to the quality control plan.

The quality control system must include all aspects of the job including mail flow and materials handling. The plan must also allow for a complete audit trail (e.g., it must be possible to locate any piece of mail at any time from the point it leaves the press up to and including the point at which the mail is off-loaded at the USPS facility). SSA will not request, as a routine matter, the contractor to produce pieces in transit within the contractor's plant.

The quality control plan must account for the number of pieces mailed daily.

Quality Control Sample Plan – The plan must provide a description of how the contractor will create quality control samples for periodic samplings to be taken during the production run and provide for backup and re-running in the event of an unsatisfactory sample. The plan must contain control systems that will detect defective, missing, or mutilated pieces.

The plan must include the sampling interval the contractor intends to utilize. The contractor will be required to create two (2) quality control samples every 4,000 notices. Mailers with low volumes (less than 4,000) will require at least one (1) set of samples to be produced. The samples are to be drawn from the production stream at the same time:

- One (1) sample will be drawn, inspected, and retained as part of the contractor's quality assurance records.

- One (1) sample will be drawn for the Social Security Administration and packed with the remaining samples associated with each print order and shipped to: Social Security Administration, Attn: Melissa Picone, Printing and Postage, 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401.

Samples must be bulk shipped to SSA weekly for each print order. The contractor must ship the quality control samples for each specific print order within two (2) workdays following the final mail date of the print order.

The plan must detail the actions to be taken by the contractor when defective, missing, or mutilated items are discovered. These actions must be consistent with the requirements found in GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987 (Rev. 01-18)).

The plan must monitor all aspects of the job, including material handling and mail flow, to assure the production and delivery of these notices meet specifications and Government requirements. This includes maintaining 100% accountability in the accuracy of imaging and mailing of all pieces throughout each run. The contractor must ensure that there are no missing or duplicate pieces.

NOTE: Contractor must submit samples of the Automated Audit Report and 100% Accountability Summary Report. (See "100% ACCOUNTABILITY OF PRODUCTION AND MAILING.")

The contractor must maintain quality control samples, inspection reports, and records for a period of no less than 210 calendar days subsequent to the date of the check tendered for final payment by the Government Publishing Office. The Government will periodically verify that the contractor is complying with the approved quality control plan through on-site examinations and/or requesting copies of the contractor's quality assurance records and quality assurance random copies.

Computer System Plan – This plan must include a detailed listing of the contractor's operating software platform and file transfer system necessary to interface with SSA's National File Transfer Management System (FTMS) for electronic transmission of files from SSA. The plan must also include the media type on which files from SSA will be received to the extent that operator intervention (e.g., a tape mount) is not required at SSA or the contractor's production facility.

The system plan must demonstrate the contractor's ability to provide complete hardware and software compatibility with SSA's existing network. (See "FILE TRANSFER MANAGEMENT SYSTEM (FTMS) REQUIRMENTS.") The contractor must complete a Computer System Plan (see Exhibit M).

Included with the Computer System Plan must be a resume for each employee responsible for the monitoring and the programming of the contractor's computer system and file transmissions. If the contractor plans to use a consultant for either task, a resume must still be included. This plan must show that the programmer(s) is skilled in the handling of record specifications and programming of the Advanced Function Presentation (Fully Composed) resources and files.

Mail Plan – This plan must include sufficient detail as to how the contractor will comply with all applicable U.S. Postal Service mailing requirements as listed in the USPS Domestic and International Mail Manuals in effect at the time of the mailing and other USPS instructional material such as the Postal Bulletin. The contractor must also disclose how they will achieve multi-level USPS automated presort postal discounts as outlined in the contract.

Material Handling and Inventory Control Plan – This plan must explain in detail how the following materials will be handled throughout all phases of production: incoming raw materials; work-in-progress materials; quality control inspection materials; USPS inspection materials; all outgoing materials cleared for USPS pickup/delivery; and method of disposal of all production waste materials.

Personnel Plan – In conjunction with the required applicant listing (See "Clause 2352.204-1 – Security and Suitability Requirements (Sept 2023)"), this plan must include a listing of all personnel who will be involved with this contract. For any new employees, the plan must include the source of these employees and a description of the training programs the employees will receive to familiarize them with the requirements of this program.

Production Plan – The contractor must provide a detailed plan of the following:

(a) List of all production equipment and equipment capacities to be utilized on this contract;
(b) The production capacity currently being utilized on this equipment;
(c) Capacity that is available for these workloads; and,
(d) If new equipment is to be utilized, documentation of the purchase order, source, delivery schedule, and installation dates are required.

The contractor must disclose in their production plan their intentions for the use of any subcontractor(s). The plan must include the same information required from the contractor for all items contained under "SECURITY REQUIREMENTS" and "PREAWARD SURVEY." If a subcontractor for any operation is added at any time after award, the contractor must submit the subcontractor's proposed plans which are subject to review and approval by the Government.

The subcontractor must be approved by the Government prior to production starting in that facility. If the subcontractor is not approved by the Government, then the contractor has 30 calendar days prior to production to submit to the Government the new subcontractor's information.

Security Control Plan – The contractor must maintain in operation an effective security system where items by these specifications are manufactured and/or stored (awaiting distribution or disposal) to assure against theft and/or the product ordered falling into unauthorized hands.

Contractor is cautioned that no Government provided information shall be used for non-government business. Specifically, no Government information shall be used for the benefit of a third party.

The Government retains the right to conduct on-site security reviews at any time during the term of the contract.

The plan shall contain at a minimum:

(1) How Government files (data) will be secured to prevent disclosure to a third party;
(2) How the disposal of waste materials will be handled (see "*Disposal of Waste Materials*");
(3) How all applicable Government-mandated security/privacy/rules and regulations as cited in this contract must be adhered to by the contractor and/or subcontractor(s);
(4) How contractors classified as Cloud Service Providers (CSP) will adhere to additional FedRAMP security control requirements. CSPs must have a security control assessment performed by a Third Party Assessment Organization (3PAO);
(5) The contractor shall submit a System Authorization Package as described in the "SSA External Service Provider Security Requirements" section. The SSP, a part of this package, documents how the solution implements security controls in accordance with the designated FIPS 199 security categorization and the Minimum Security Requirements for Federal Information and Information Systems. This SSP requires the use of NIST SP 800-53 v4. The SAP should be completed by either an independent assessor or another Federal agency.

Production Area Plan – The contractor must provide a secure area(s) dedicated to the processing and storage of data for the notices, either a separate facility dedicated to these products, or a walled-in, limited access area within the contractor's existing facility. Access to the area(s) must be limited to security-trained employees involved in the production of the notices.

Part of the Production Area Plan must include a floor plan detailing the area(s) to be used, showing existing walls, equipment to be used, and the printing and finishing locations.

Contractor must have, in place, a building security system that is monitored 24 hours a day, seven (7) days a week, and a badging/keypunch system that limits access to Government materials (data processing center/production facility and other areas where Government materials with PII are stored or are accessible) that is only accessible by approved personnel. Contractor must present this information, in detail, in the production area plan.

Disposal of Waste Materials – The contractor is required to demonstrate how all waste materials used in the production of sensitive SSA records (records containing PII information as identified in "SECURITY WARNING") will be definitively destroyed (e.g., burning, pulping, shredding, macerating, or other suitable similar means). Electronic Records must be definitively destroyed in a manner that prevents reconstruction. *Sensitive* records are records that are national security classified or exempted from disclosure by statue, including the Privacy Act or

regulation. *Definitively* destroying the records means the material cannot be reassembled and used in an inappropriate manner in violation of law and regulations.

The contractor, at a minimum, must crosscut shred all documents into squares not to exceed one-quarter inch. All documents to be destroyed cannot leave the security of the building, must be destroyed at contractor's printing site, and cannot be subcontracted. The contractor must specify the method planned to dispose of the material.

UNIQUE IDENTIFICATION NUMBER: Unique identifying numbers will be used to track each individual notice, thereby providing 100% accountability. This enables the contractor to track each notice through completion of the project. The contractor will be required to create a test sample every 4,000 notices. Each file must have a minimum of one (1) test sample. This sample must have a unique number and must be produced on each notice. The contractor will generate a list of the unique identifying numbers for each sample. As samples are pulled, the unique numbers will be marked off the list. This enables the contractor to track which samples have been produced and pulled and what records have been produced.

The contractor may create their own sequence number and run date to facilitate their presorting and inserting process but must maintain the original SSA identification number.

RECOVERY SYSTEM: A recovery system will be required to ensure that all defective, missing, or mutilated pieces detected are identified, reprinted, and replaced. The contractor's recovery system must use the unique sequential alpha/numeric identifiers assigned to each piece (including quality control samples) to aid in the recovery and replacement of any defective, missing, or mutilated pieces, and must be capable of tracking and/or locating any individual piece of mail from the time it leaves the press, up to and including when it is off-loaded at the U.S. Postal Service facility. An explanation of the contractor's sequential numbering system is required to understand the audit trail required for each and every piece.

100% ACCOUNTABILITY OF PRODUCTION AND MAILING: Contractor must have a closed loop process* to determine that the data from the original print file is in the correct envelope with the correct number of pages. Notices requiring print regeneration must be reprinted from their original print image with the original job ID and piece ID remaining unchanged as each mail piece continues through the inserting life cycle. This process will repeat itself (since subsequent reprint runs may yield damages) until all mail pieces from the original print run have been inserted and accounted for.

***Closed Loop Processing* –** A method for generating a plurality of mail pieces including error detection and reprinting capabilities. The method provides a mail handling process, which tracks processing errors with the use of a first and second scan code, which obtain information regarding each mail piece, diverts mail pieces in response to error detection, transmits such errors to a processor, and automatically generates a reconfigured print file to initiate reprints for the diverted mail pieces.

Contractor will be responsible for providing a unique identifying number that will be used to track each individual notice, thereby providing 100% accountability and validating the integrity of every notice produced in all phases of printing, inserting, and mailing, and to ensure all notices received from SSA were correctly entered into the U.S. Postal System.

NOTE: Contractor must have all hardware, programming, and finalized reports in place to meet this requirement. The equipment must arrive, be installed, and be fully functional at least 120 calendar days prior to the start of live production on September 1, 2027. Contractor must submit a sample of their proposed Audit and Summary Reports with the required Preaward Production Plans for approval. The Government considers grounds for the immediate default of this contract if the contractor, at any time, is unable to perform or found not complying with any part of this requirement.

Notice integrity shall be defined as follows:

- Each notice must include all pages (and only those pages) intended for the designated recipient as contained in the print files received from SSA.

- The contractor's printing process must have automated systems which can detect all sync errors, stop printing when detected, and identify, remove, and reprint all effected notices.

Mailing integrity shall be defined as follows:

- All notices received from SSA for each file date were printed, inserted, and entered correctly into the U.S. Postal System.

The contractor is responsible for providing the automated inserted notice tracking/reporting systems and processes required to validate that 100% of all notices received from SSA were printed, all pages for each notice are accounted for, inserted, and mailed correctly.

The contractor's inserting equipment must have automated systems that include notice coding and scanning technology capable of:

(a) Uniquely identifying each notice and corresponding notice leaves within each individual file by mailer number and file date.

(b) Unique identifier to be scanned during insertion to ensure all notices and corresponding notice leaves are present and accounted for.

(c) *Entrance Scanning:* A camera system must electronically track and scan all leaves of each mail piece as the inserting equipment pulls them into the machine to ensure each mail piece was produced and inserted. If there is any variance on a mail piece or if a mail piece is not verified that all leaves are present, that piece and the piece prior to and immediately following must be diverted and sent back for reprint. All instances of variance must be logged.

(d) *Touch and Toss:* All spoilage, diverted, mutilated, or mail pieces that are acted upon directly by a human hand prior to sealing must be immediately recorded, discarded, properly destroyed, and automatically regenerated in a new print file for reprint. *Exception* – Intentionally diverted pieces due to a requirement for a product, which cannot be intelligently inserted and requires manual insertion such as a publication, can be sealed, rescanned, and placed back into production. These must be programmed diverts and sent to a separate bin for processing to ensure they are not mixed with other problem diverts and logged into the Audit system as such.

(e) *Exit Scanning:* A camera system must be mounted just aft of the inserting equipment. This camera system must read a unique code through the window of each mail piece and be capable of identifying and reporting all missing notices that were lost or spoiled during production for each individual file by mailer number and file date. This system must ensure that no missing mail pieces have been inadvertently inserted into another mail piece. The equipment must check the mail pieces after insertion, verify that all leaves are accounted for, and divert any suspect product. During exit scanning, if a sequence number is missing, the notice prior to and immediately after must be diverted. The equipment must divert all products that exhibit missing or out of order sequence numbers and any other processing errors. All diverted pieces are to be automatically recorded and regenerated in a new print file for reprint.

(f) *Reconciliation:* All notices and the amount of correct finished product must be electronically accounted for after insertion through the use of the audit system that is independent of the inserting equipment as well as independent of the operator. The sequence numbers for each file must be reconciled, taking into account

any spoilage, duplicate, and/or diverted product. If the reconciliation yields divergent results, corrective action must be taken to locate the mail pieces that are causing any difference between the input and outputs of the inserting process. Therefore, all finished mail for that sequence run must be held in an accessible area until this reconciliation is complete.

(g) Generate a new production file for all missing, diverted, or mutilated notices (reprint file).

(h) Contractor must generate an Automated Audit Report from the information gathered from scanning for each mailer number, file date, and each notice (manual inputs are not allowed). This audit report will contain detailed information for each notice as outlined above for each individual file by mailer number and file date. Contractor must maintain this information for 210 calendar days after mailing.

(i) Audit report must contain the following information:

1. Job name
2. Mailer number, file date, and mail date(s)
3. Machine ID
4. Date of production with start and end dates and times for each phase of the run (i.e., machine ID).
5. Start and end sequence numbers in each run
6. Status of all sequence numbers in a run
7. Total volume in run
8. Status report for all incidents for each sequence number and cause (e.g., inserted, diverted, and reason for diverting such as missing sequence number, missing leaves, mutilated, duplicate, pulled for inspection, etc.).
9. Bottom of audit report must contain total number of records for that run, quantity sent to reprint, number of duplicates, duplicates verified and pulled, and total completed.
10. Audit report must contain the same information for all the reprints married with this report as listed above showing that all pieces for each mailer number and file date are accounted for with corresponding date stamp of completion of each.

(j) Contractor must generate a final automated 100% Accountability Summary Report for each individual file by mailer number and file date. This information must be generated directly from the audit report. Manual inputs are not allowed. The 100% Accountability Summary Report must contain the following:

1. Job information - Job name, file date, mailer number, piece quantity, sequence start and end numbers, if multiple batches for a single file include number of batches and batch number (i.e., 1 of 4, due date, etc.).
2. Job Start Time and Job End Time
3. Volume of sequence numbers associated with an individual file by mailer number and file date that were inserted and date completed.
4. Volume of reprints that were inserted for each file date and when completed.
5. Total volume inserted for each file date and final date and time that each batch was completed.

A PDF copy of the summary report(s) and matching USPS Certificate of Bulk Mailing, USPS 3607R and/or GPO 712 form(s) must be emailed to Melissa Picone at melissa.picone@ssa.gov within two (2) workdays of mailing. All USPS mailing documents must be labeled with file date, mailer ID, and the job ID, as noted in the supplied files.

Contractor must submit a sample of their Audit and Summary Reports (see Exhibit N) with the required Preaward Production Plans for Government review and approval. The audit team must approve the audit and summary reports prior to award. During the term of the contract, NO changes are to be made to the approved audit and summary reports without prior approval from the audit team. The contractor must submit in writing a request to make changes to the audit and summary reports, along with samples of the proposed audit and summary reports for review and approval.

Contractor must generate an automated audit report when necessary showing the tracking of all notices throughout all phases of production for each mail piece. This audit report will contain all information as outlined in item (i) above. Contractor is required to provide any requested Summary and/or Audit reports within one (1) hour of a request via email in an MS Word, MS Excel, or PDF file to Melissa Picone at melissa.picone@ssa.gov.

NOTE: The Government reserves the right to conduct an audit at any time during the term of the contract. The audit team will provide the contractor a minimum of a 24-hour notice prior to audit. If the contractor produces multiple SSA contracts, the audit team will provide a list of contracts and print orders they will require full audit reports, summary reports, and postal documentation for during the audit.

The contractor must provide the required audit reports within one (1) hour of request; the audit team will grant one (1) hour for each report to be pulled. The audit team may request a full tour and demonstration of the accountability process at the time of the audit. A wrap-up meeting will occur at the conclusion of the audit. The audit team will review their findings with the contractor at this time. The contractor will need to provide in writing responses to all findings, questions, and concerns within one (1) week of the wrap-up meeting. If corrections are required to the contractor's audit reports, the Government may grant the contractor 60 calendar days to complete the changes. The audit team must approve the audit and summary report changes prior to the contractor implementing the changes.

Once the new report is approved, the contractor must update the sample of the audit and summary reports provided with the production plans. The Government considers grounds for the immediate default of this contract if the contractor, at any time, is unable to perform or found not in compliance with any part of this requirement.

All notice tracking/reporting data must be retained in electronic form for 210 calendar days after mailing and must be made available to SSA for auditing of contractor performance upon request.

NOTE: The Government will not as a routine matter request the contractor produce individual pieces in transit within the plant; however, the contractor must demonstrate that they will have an audit trail established that has the ability to comply with this type of request when and if the need arises.

REQUEST FOR NOTICE PULLS FROM PRODUCTION: Due to the sensitivity of the notices in this contract, the Government may request that certain notices be removed from the production stream. When this occurs, the Government will supply the contractor with a list of the notices that need to be pulled.

The contractor must be able to run a sort to find and eliminate the notice from the production run. If the list is provided after the notice has been produced, the contractor must be capable of identifying the notice and pulling it from the production floor. It is anticipated that this will be an infrequent occurrence.

REQUEST FOR FOREIGN NOTICE PULLS FROM FILE PRIOR TO PRODUCTION: The contractor is to remove foreign notices from files transmitted prior to production of the files. The contractor must email Melissa Picone at melissa.picone@ssa.gov each week with the total number of foreign notices pulled from each mailer. The email should include the number of notices pulled, the mailer number, and the file name with the file date (e.g., M2S, 1 record in file "MMAPPNOT.VEND1SP.R260403").

ON-SITE REPRESENTATIVES: One (1) or two (2) full-time Government representatives may be placed on the contractor's premises on a limited basis or throughout the term of the contract.

The contractor will be required to provide one private office of not less than 150 square feet, furnished with at least one desk, two swivel armchairs, secure internet access for Government laptop computers, a worktable, and two 4-drawer letter-size file cabinets with combination padlock and pendaflex file folders or equal.

On-site representative(s) may be stationed at the contractor's facility to: provide project coordination in receipt of transmissions; verify addresses; monitor the printing, imaging, folding, inserting, mail processing, quality control, sample selections, and inspections; and, monitor the packing and staging of the mail.

These representatives will not have contractual authority and cannot make changes in the specifications or in contract terms but will bring defects detected to the attention of the company Quality Control Officer. The representatives must have full and unrestricted access to all production areas where work on this program is being performed.

POSTAWARD CONFERENCE: Unless waived by the Contracting Officer, the total requirements of the job as indicated in these specifications will be reviewed by Government representatives with the contractor's representatives at the Social Security Administration, Baltimore, MD, immediately after award. At the Government's option, the postaward conference may be held via teleconference.

Person(s) that the contractor deems necessary for the successful implementation of the contract must be in attendance.

PREPRODUCTION MEETING: A preproduction meeting covering the printing, imaging, folding, inserting, and mailing will be held at the contractor's facility after award of the contract to review the contractor's production plan and to establish coordination of all operations. Attending this meeting will be representatives from the Government Publishing Office, Social Security Administration, and U.S. Postal Service. The contractor must present and explain their final plan for the printing, imaging, folding, inserting, and mailing of all notices.

At the Government's option, the preproduction meeting may be held via teleconference. The Government reserves the right to waive the preproduction meeting.

The contractor shall meet with SSA and USPS representatives to present and discuss their plan for mailing. The preproduction meeting may include a visit to the contractor's mailing facility where the contractor is to furnish specific mail flow information.

The contractor must present documentation of the plant loading agreement and either a copy of the optional procedure, which has been negotiated with the USPS or a draft of the original procedure that the contractor intends to negotiate with the USPS for SSA approval. The contractor also needs to present SSA with a copy or a draft of the manifest (tracking system) to be used to accomplish the above.

In addition, the contractor must be prepared to present detailed production plans, including such items as quality assurance, projected commencement dates, equipment loading, pallet needs, etc. The contractor is to provide the name of the representative responsible for the mailing operation and that individual's backup.

Person(s) that the contractor deems necessary for the successful implementation of the contract must be in attendance.

ASSIGNMENT OF JACKET, PURCHASE ORDER, AND PRINT ORDERS: A GPO jacket number will be assigned and a purchase order issued to the contractor to cover the work performed. The purchase order will be supplemented by an individual print order for each job placed with the contractor. The print order, when issued, will indicate the quantity to be produced and any other information pertinent to the order.

ORDERING: Items to be furnished under the contract must be ordered by the issuance of weekly print orders supplemented by daily electronic notice counts. Orders may be issued under the contract from March 1, 2027 through February 29, 2028, plus four such additional period(s) as the contract is extended. All print orders issued hereunder are subject to the terms and conditions of the contract. The contract shall control in the event of conflict with any print order or electronic notice count.

Notice counts will be "issued" daily via email for purposes of the contract and will detail the daily volume of notices required. A print order (GPO Form 2511) will be used for billing purposes, issued weekly, and will cover all daily electronic transmissions sent during that week. A print order shall be "issued" upon notification by the Government for purposes of the contract when it is electronically transmitted or otherwise physically furnished to the contractor in conformance with the schedule.

REQUIREMENTS: This is a requirements contract for the items and for the period specified herein. Shipment/delivery of items or performance of work shall be made only as authorized by orders issued in accordance with the clause entitled "ORDERING." The quantities of items specified herein are estimates only and are not purchased hereby. Except as may be otherwise provided in this contract, if the Government's requirements for the items set forth herein do not result in orders in the amounts or quantities described as "estimated," it shall not constitute the basis for an equitable price adjustment under this contract.

Except as otherwise provided in this contract, the Government shall order from the contractor all the items set forth which are required to be purchased by the Government activity identified on page 1.

The Government shall not be required to purchase from the contractor, requirements in excess of the limit on total orders under this contract, if any.

Orders issued during the effective period of this contract and not completed within that time shall be completed by the contractor within the time specified in the order, and the rights and obligations of the contractor and the Government respecting those orders must be governed by the terms of this contract to the same extent as if completed during the effective period of this contract.

If shipment/delivery of any quantity of an item covered by the contract is required by reason of urgency prior to the earliest date that shipment/delivery may be specified under this contract, and if the contractor will not accept an order providing for the accelerated shipment/delivery, the Government may procure this requirement from another source.

The Government may issue orders which provide for shipment/delivery to or performance at multiple destinations.

Subject to any limitations elsewhere in this contract, the contractor shall furnish to the Government all items set forth herein which are called for by print orders issued in accordance with the "ORDERING" clause of this contract.

PRIVACY ACT NOTIFICATION: This procurement action requires the contractor to do one or more of the following: design, develop, or operate a system of records on individuals to accomplish an agency function in accordance with the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties as stated in 5 U.S.C. 552a (i)(1) CRIMINAL PENALTIES. It is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a, specifically, 5 U.S.C. 552a (i)(1) CRIMINAL PENALTIES and m(1) GOVERNMENT CONTRACTORS.

PRIVACY ACT

(a) The contractor agrees:

(1) to comply with the Privacy Act of 1974 and the rules and regulations issued pursuant to the Act in the design, development, or operation of any system of records on individuals in order to accomplish an agency function when the contract specifically identifies (i) the system or systems of records and (ii) the work to be performed by the contractor in terms of any one or combination of the following: (A) design, (B) development, or (C) operation;

(2) to include the solicitation notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation when the statement of work in the proposed subcontract requires the design, development, or operation of a system of records on individuals to accomplish an agency function; and

(3) to include this clause, including this paragraph (3), in all subcontracts awarded pursuant to this contract which require the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved where the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency where the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor and any employee of the Contractor is considered to be an employee of the agency.

(c) The terms used in this clause have the following meanings:

(1) "Operation of a system of records" means performance of any of the activities associated with maintaining the system of records including the collection, use, and dissemination of records.

(2) "Record" means any item, collection or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

(3) "System of records" on individuals means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

ADDITIONAL EMAILED BID SUBMISSION PROVISIONS: The Government will not be responsible for any failure attributable to the transmission or receipt of the emailed bid including, but not limited to, the following:

1. Illegibility of bid.
2. Emails over 75 MB may not be received by GPO due to size limitations for receiving emails.
3. The bidder's email provider may have different size limitations for sending email; however, bidders are advised not to exceed GPO's stated limit.
4. When the email bid is received by GPO, it will remain unopened until the specified bid opening time. Government personnel will not validate receipt of the emailed bid prior to bid opening. GPO will use the prevailing time (specified as the local time zone) and the exact time that the email is received by GPO's email server as the official time stamp for bid receipt at the specified location.

PAYMENT: Submitting invoices for payment via the GPO fax gateway (if no samples are required) utilizing the GPO barcode coversheet program application is the most efficient method of receiving payment. Instruction for using this method can be found at the following web address:
http://winapps.access.gpo.gov/fms/vouchers/barcode/instructions.html.

Invoices may also be mailed to: U.S. Government Publishing Office, Office of Financial Management, Attn: Comptroller, Stop: FMCE, Washington, DC 20401.

For more information about the billing process, refer to the General Information of the Office of Finance web page located at: https://www.gpo.gov/how-to-work-with-us/vendors/how-to-get-paid.

Contractor's billing invoice must be itemized in accordance with the items in the "SCHEDULE OF PRICES."

SECTION 2. - SPECIFICATIONS

SCOPE: These specifications cover the production of mailing packages from four (4) identified workloads (total of 10 mailers) consisting of English or Spanish personalized scannable forms; English or Spanish personalized worksheets; English or Spanish personalized letters; Business Reply Mail (BRM) return envelopes, and mail-out envelopes requiring such operations as: the receipt and processing of transmitted data; composition; printing; imaging (computerized printing); binding; construction; gathering and inserting; packing; and distribution.

In addition, these specifications cover the production of bulk mailers 1BL and 2BL consisting of an English or Spanish non-personalized scannable form (containing a 2D barcode), a Business Reply Mail (BRM) return envelope, and a mail-out envelope requiring such operations as composition, printing, binding, construction, gathering and inserting, packing, and bulk shipment delivery.

TITLE: Medicare (Part D Subsidy) Notices.

The four (4) identified workloads are as follows:

1. New Attainers
2. Subsidy Changing Event (SCE)
3. Redetermination (REDE)
4. CMS Letter

NOTE: These specifications also include a Bulk Mailer Requirement for Bulk Form 1BL and 2BL.

Future Workloads (during term of contract): During the term of this contract, the Government anticipates developing new notice workloads with the same or similar requirements as the mailing packages described by these specifications. All terms and conditions in these specifications will apply to any future notice workloads. It is estimated that approximately one (1) to three (3) new notice workloads may be added during the term of this contract. File names/dataset names for the new mailers will be supplied to the contractor as they are developed.

FREQUENCY OF ORDERS:

A weekly print order will be issued for each week's file transmissions, indicating the total quantity to be produced. The print order will be supplemented by daily electronic notice counts provided via email.

Below is an anticipated transmission schedule. Delays and changes to the schedule may occur. Contractor must be prepared to receive files 24/7/365.

- Mailers 1, 2, 3, 4, 5, 6, 8, 9, and 10 will transmit daily.
- Mailers 1, 2, and 8 New Attainers SPIKE will transmit between the 24th and 28th of each month.
- Mailers 5, 6, and 10 REDE SPIKE will transmit in one (1) session on the Monday before Labor Day in August of each year. The REDE SPIKE represents the majority of the annual Redetermination quantity. Subsequent quantities will be minimal to none.
- Mailer 7 will transmit in one (1) session no later than the Friday after Labor Day in September of each year. Mailer 7 includes an English or Spanish CMS Letter and the SSA-1020B-OCR-SM or SSA-1020B-OCR-SM-SP form. The record layout provided for Mailer 7 contains information specific to this mailer only. A separate Excel spreadsheet listing the CMS toll-free numbers for each state will be provided for use in the CMS letter. An electronic version of the CMS Letter will be available in July of each year.

- Bulk Mailer Requirement: Approximately one (1) or two (2) print orders will be issued each year for Bulk Mailers 1BL and 2BL. One order will be placed in December, and, if required, a second order may be placed around mid-year. Bulk Mailers 1BL and 2BL may be included on the same print order or on separate print orders.

  NOTE: The contractor must provide daily production reports in Excel format for the REDE SPIKE and CMS Mailer 7. The report must show the quantity of notices printed, inserted, and mailed, as well as the number remaining for each process. The Government may request production reports at any time for any notice covered by this contract.

For the initial composition and proofs, SSA will send an email (along with the furnished copy) ordering the composition and proofs. Multiple rounds of proofs may be required. Upon receipt of "O.K. to Print" on the proofs, the composition and proofs will be ordered on the same print order as the construction samples validation test.

A separate print order will be issued for the following tests:

- Transmission Test
- Preproduction Validation Test
- Construction Samples Validation Test
- Preproduction Press and Mail Run Test

Throughout the term of the contract, all required proofs and the Systems Change/New and Existing Notice Files Validation Test will be ordered on a live production print order.

QUANTITY:

Mailers 1 through 10: The combined yearly total for all mailers is approximately 3,451,800 notices per year, broken down as follows:

- New Attainers: Approximately 2,220,000 notices.
  - M1: 2,069,650
  - M2: 150,000
  - M8: 350
- Subsidy Changing Event (SCE): Approximately 7,800 notices.
  - M3: 7,070
  - M4: 725
  - M9: 5
- Redetermination (REDE): Approximately 224,000 notices.
  - M5: 206,500
  - M6: 17,350
  - M10: 150
- CMS Letter: Approximately 1,000,000 notices
  - M7 English: 920,000
  - M7 Spanish: 80,000

The Government reserves the right to increase or decrease the quantity by up to 25% of the total number of notices ordered annually. Exact quantities will be furnished with the electronic file. This 25% includes the additional notices occasioned by the one (1) to three (3) new notice workloads that may be added during the term of this contract.

Bulk Mailers: The combined yearly total for all Bulk Mailers (1BL and 2BL) is approximately 1,350,000 mailers per year, broken down as follows:

- Bulk Mailer Requirement: Approximately 350,000 mailers.
  - 1BL: 315,000
  - 2BL: 35,000
- CMS M7 Insert: Approximately 1,000,000 mailers.
  - 1BL: Approximately 920,000
  - 2BL: Approximately 80,000

The Government reserves the right to increase or decrease the quantity by up to 25% of the total number of Bulk Mailers ordered annually. Exact quantities will not be known until ordered.

90-CALENDAR DAY VOLUMES:

New Attainers:

Mail-out Envelopes (6-1/8 x 9-1/4"):		90-Calendar Day Estimated Volumes
SSA-1020-OCR-SM	PO BOX 1020	517,412
SSA-1020-OCR-SM-SP	PO BOX 1020	37,500
BRM Envelopes (5-3/4 x 8-3/4"):		
SSA-1020-OCR-SM	PO BOX 1020	517,412
SSA-1020-OCR-SM-SP	PO BOX 1020	37,500

Subsidy Changing Event (SCE):

Mail-out Envelopes (6-1/8 x 9-1/4"):		90-Calendar Day Estimated Volumes
SSA-1026-OCR-SM-SCE	PO BOX 1080	1,768
SSA-1026-OCR-SM-SCE-SP	PO BOX 1080	182
BRM Envelopes (5-3/4 x 8-3/4"):		
SSA-1026-OCR-SM-SCE	PO BOX 1080	1,768
SSA-1026-OCR-SM-SCE-SP	PO BOX 1080	182

Redetermination (REDE):

Mail-out Envelopes (6-1/8 x 9-1/4"):		90-Calendar Day Estimated Volumes
SSA-1026-OCR-SM-REDE	PO BOX 1080	51,625
SSA-1026-OCR-SM-REDE-SP	PO BOX 1080	4,338
BRM Envelopes (5-3/4 x 8-3/4"):		
SSA-1026-OCR-SM-REDE	PO BOX 1080	51,625
SSA-1026-OCR-SM-REDE-SP	PO BOX 1080	4,338

CMS Letter:

The CMS Letter is an annual notice. All components required for the CMS Letter are excluded from the 90-calendar day surplus/inventory.

NUMBER OF PAGES AND TRIM SIZES:

Notices	No. of Pages	Trim Size
Scannable Forms:	8 pages (2 leaves)	16-3/4 x 10-3/4" flat (folded to 8-3/8 x 10-3/4")
Worksheets:	2 pages (1 leaf)	8-1/2 x 11"
Letters:	4 pages (2 leaves)	8-1/2 x 11"

Envelopes	No. of Pages	Trim Size
BRM Envelopes:	Face and back	5-3/4 x 8-3/4", plus flap
Mail-out Envelopes (Window):	Face and back	6-1/8 x 9-1/4", plus flap
Mail-out Envelopes (Non-Window):	Face and back	6-1/8 x 9-1/4", plus flap

NOTES:
1) The trim sizes for the envelopes are after manufacturing.
2) The scannable forms produced under these specifications require precision spacing, printing, trimming, and folding to guarantee proper processing.

GOVERNMENT TO FURNISH:

Manuscript copy for all notices (including eight (8) forms, four (4) worksheets, and two (2) CMS Letters).

Manuscript copy for nine (9) mail-out envelopes and nine (9) BRM return envelopes.

Vendor/Record Specifications via email.

Camera copy or electronic files via email for the SSA and CMS logos.

At the Government's option, camera copy or electronic files (PostScript format) for the recycled paper logo and legend (English and Spanish) may be furnished.

Camera copy for the Facing Identification Mark (FIM) and ZIP+4 Intelligent Mail Barcode (IMb) required for the BRM envelopes.

Coding Accuracy Support System (CASS) Certificate.

National Change of Address (NCOA) Certificate.

PS Form 3615 (Mailing Permit Application and Customer Profile): one for SSA; one for CMS.

Mailing Indicia ("Postage and Fees Paid").

A data connection between the contractors specified location and the nearest available SSA network interface location or SSA's National Computer Center in Baltimore, MD.

Identification markings such as register marks, commercial identification marks of any kind, etc., except GPO imprint, form number, and revision date, carried in the furnished electronic files or furnished copy, must not print on the finished product.

EXHIBITS:

Exhibit A: Contractor Personnel Security Certification (Form SSA 301)
Exhibit B: NIST Special Publication 800-171r3, CUI-SSP Template
Exhibit C: NIST Special Publication 800-53r5, System Security Plan (SSP) Template
Exhibit D: NIST Special Publication 800-171r3, System Security Plan (SSP)
Exhibit E: SSA PII Loss Reporting Template
Exhibit F: General Records Schedule 4.2, Information Access and Protection Records, Item 40
Exhibit G: Declaration for Federal Employment (Optional Form 306)
Exhibit H: Questionnaire for Public Trust Positions (Standard Form (SF) 85P)
Exhibit I: Fingerprint Card (FD-258)
Exhibit J: Contractor Personnel Rollover Request Form
Exhibit K: Form SSA-222
Exhibit L: Cybersecurity Supply Chain Assessment (CSCRA) Questionnaire
Exhibit M: Computer System Plan
Exhibit N: Audit and Summary Reports

CONTRACTOR TO FURNISH: All materials and operations, other than those listed under "GOVERNMENT TO FURNISH," necessary to produce the product(s) in accordance with these specifications.

Secure File Transfer Protocols (SFTP) Site: Contractor is required to set up, establish, and maintain a contractor-hosted SFTP website that multiple users at SSA can access for passing PDF notice validation samples and other information that contains PII to SSA and back. SFTP website must be accessible via Edge web browser and must not require the download or installation of any additional software. (NOTE: Contractor cannot send any notices or information that contain PII via email.) Appropriate log-on instructions and protocol must be provided by the contractor at time of award. The contractor shall provide security, which at a minimum, shall require a unique user ID and password for each user to access.

DATASET NAMES: The dataset names listed below may not be the final dataset names transmitted to the contractor. If there are changes, final dataset names will be provided to the contractor at the postaward conference.

WORKLOAD	MAILER	DATASET NAME
New Attainers	1	OLBG.BTI.*vendo*r.MMAPPNOT.VEND101.*ryymmdd*
		OLBG.BTI.*vendo*r.MMAPPNOT.VEND1RR.*ryymmdd*
	2	OLBG.BTI.*vendo*r.MMAPPNOT.VEND1SP.*ryymmdd*
Subsidy Changing Event (SCE)	3	OLBG.BTI.*vendor*.MMSCENOT.VEND101.*ryymmdd*
		OLBG.BTI.*vendor*.MMSCENOT.VEND1RR.*ryymmdd*
	4	OLBG.BTI.*vendor*.MMSCENOT.VEND1SP.*ryymmdd*
Redetermination (REDE)	5	OLBG.BTI.*vendor*.MMREDNOT.VEND101.*ryymmdd*
		OLBG.BTI.*vendor*.MMREDNOT.VEND1RR.*ryymmdd*
	6	OLBG.BTI.*vendor*.MMREDNOT.VEND1SP.*ryymmdd*
CMS Letter	7	OLBG.CFI.*vendo*r.AMRS.UNDEEMED.*ryymmdd*

Certified Mailers: Contractor will be required to mail Certified Mailers 8, 9, and 10 in accordance with the USPS regulations contained in the Domestic Mail Manual (DMM) under section 503.3.0, Certified Mail. (see "USPS Certified Mail" for additional information.)

New Attainers	8	OLBG.BTI.*vendo*r.MMAPPNOT.MEDCRTEN.*ryymmdd* OLBG.BTI.*vendo*r.MMAPPNOT.MEDCRTRR.*ryymmdd* OLBG.BTI.*vendo*r.MMAPPNOT.MEDCRTSP.*ryymmdd*
Subsidy Changing Event (SCE)	9	OLBG.BTI.*vendor*.MMSCENOT.MEDCRTEN.*ryymmdd* OLBG.BTI.*vendor*.MMSCENOT.MEDCRTRR.*ryymmdd* OLBG.BTI.*vendor*.MMSCENOT.MEDCRTSP.*ryymmdd*
Redetermination (REDE)	10	OLBG.BTI.*vendor*.MMREDNOT.MEDCRTEN.*ryymmdd* OLBG.BTI.*vendor*.MMREDNOT.MEDCRTRR.*ryymmdd* OLBG.BTI.*vendor*.MMREDNOT.MEDCRTSP.*ryymmdd*

In the production file, the RYYMMDD represents the file run date. For example, if the notices are scheduled to run on September 14, 2027 (with a run date of 09/14/27), the RYYMMDD portion of the file name will be "R270914."

MAKE-UP OF MAILERS: A record containing variable data will be transmitted for each mailing address. Each record will contain all variable data relevant to that address. Any alteration of the notice content in the file is not permitted.

NOTES:
1) Mailers 1, 2, 3, 4, 5, 6, 7, 1BL, and 2BL have their own version of the mail-out and BRM envelopes.
2) Mailer 8 certified uses the same envelopes as Mailer 1 or 2 (as applicable for English or Spanish).
3) Mailer 9 certified uses the same envelopes as Mailer 3 or 4 (as applicable for English or Spanish).
4) Mailer 10 certified uses the same envelopes as Mailer 5 or 6 (as applicable for English or Spanish).

Personalized Mailers: The components of each mailer are as follows:

Mailer 1	Personalized English Scannable Form (SSA-1020-OCR-SM) BRM Return Envelope (PO Box 1020) Mail-out Envelope (Window)
Mailer 2	Personalized Spanish Scannable Form (SSA-1020-OCR-SM-SP) BRM Return Envelope (PO Box 1020) Mail-out Envelope (Window)
Mailer 3	Personalized English Worksheet (SSA-1026-OCR-SM-SCE) Personalized English Scannable Form (SSA-1026-OCR-SM-SCE) BRM Return Envelope (PO Box 1080) Mail-out Envelope (Window)
Mailer 4	Personalized Spanish Worksheet (SSA-1026-OCR-SM-SCE-SP) Personalized Spanish Scannable Form (SSA-1026-OCR-SM-SCE-SP) BRM Return Envelope (PO Box 1080) Mail-out Envelope (Window)
Mailer 5	Personalized English Worksheet (SSA-1026-OCR-SM-REDE) Personalized English Scannable Form (SSA-1026-OCR-SM-REDE) BRM Return Envelope (PO Box 1080) Mail-out Envelope (Window)
Mailer 6	Personalized Spanish Worksheet (SSA-1026-OCR-SM-REDE-SP) Personalized Spanish Scannable Form (SSA-1026-OCR-SM-REDE-SP) BRM Return Envelope (PO Box 1080) Mail-out Envelope (Window)

Mailer 7 Personalized CMS English Letter (11198)
Non-Personalized English Scannable Form (SSA-1020B-OCR-SM)
BRM Return Envelope (PO Box 1021)
Mail-out Envelope (Window)

or

Personalized CMS Spanish Letter (11198-S)
Non-Personalized Spanish Scannable Form (SSA-1020B-OCR-SM-SP)
BRM Return Envelope (PO Box 1021)
Mail-out Envelope (Window)

NOTE: Mailer 7 English uses the same bulk form (SSA-1020B-OCR-SM) as 1BL. Mailer 7 Spanish uses the same bulk form (SSA-1020B-OCR-SM-SP) as 2BL.

Certified Mailers:

Mailer 8 Personalized English Scannable Form (SSA-1020-OCR-SM)
BRM Return Envelope (PO Box 1020)
Mail-out Envelope (Window)

or

Personalized Spanish Scannable Form (SSA-1020-OCR-SM-SP)
BRM Return Envelope (PO Box 1020)
Mail-out Envelope (Window)

Mailer 9 Personalized English Worksheet (SSA-1026-OCR-SM-SCE)
Personalize English Scannable Form (SSA-1026-OCR-SM-SCE)
BRM Return Envelope (PO Box 1080)
Mail-out Envelope (Window)

or

Personalized Spanish Worksheet (SSA-1026-OCR-SM-SCE-SP)
Personalized Spanish Scannable Form (SSA-1026-OCR-SM-SCE-SP)
BRM Return Envelope (PO Box 1080)
Mail-out Envelope (Window)

Mailer 10 Personalized English Worksheet (SSA-1026-OCR-SM-REDE)
Personalized English Scannable Form (SSA-1026-OCR-SM-REDE)
BRM Return Envelope (PO Box 1080)
Mail-out Envelope (Window)

or

Personalized Spanish Worksheet (SSA-1026-OCR-SM-REDE-SP)
Personalized Spanish Scannable Form (SSA-1026-OCR-SM-REDE-SP)
BRM Return Envelope (PO Box 1080)
Mail-out Envelope (Window)

Non-Personalized Bulk Mailers: The components of each bulk mailer are as follows:

1BL Non-Personalized English Scannable Form (SSA-1020B-OCR-SM)
BRM Return Envelope (PO Box 1020)
Mail-out Envelope (Non-Window)

2BL Non-Personalized Spanish Scannable Form (SSA-1020B-OCR-SM-SP)
BRM Return Envelope (PO Box 1020)
Mail-out Envelope (Non-Window)

Personalized Mailers: The figures indicated below are estimates based on historical data. They represent the minimum and maximum quantities required daily for the Medicare Notices, the minimum and maximum SPIKE quantities, the number of printed pages in a notice, and how the notice is to be folded. Exact quantities will not be known until each run is electronically transmitted to the contractor. NO SHORTAGES WILL BE ALLOWED.

Mailer 1	Daily Minimum:	0
(SSA-1020-OCR-SM)	Daily Maximum:	10,000
	SPIKE Minimum:	60,000
	SPIKE Maximum:	90,000
	Printed Pages:	8
	Folding:	Bifold
Mailer 2	Daily Minimum:	0
(SSA-1020-OCR-SM-SP)	Daily Maximum:	600
	SPIKE Minimum:	5,000
	SPIKE Maximum:	8,000
	Printed Pages:	8
	Folding:	Bifold
Mailer 3	Daily Minimum:	0
(SSA-1026-OCR-SM-SCE)	Daily Maximum:	80
	Printed Pages:	10
	Folding:	Bifold
Mailer 4	Daily Minimum:	0
(SSA-1026-OCR-SM-SCE-SP)	Daily Maximum:	20
	Printed Pages:	10
	Folding:	Bifold
Mailer 5*	Daily Minimum:	0
(SSA-1026-OCR-SM-REDE)	Daily Maximum:	3
	SPIKE Minimum:	200,000
	SPIKE Maximum:	224,000
	Printed Pages:	10
	Folding:	Bifold
Mailer 6*	Daily Minimum:	0
(SSA-1026-OCR-SM-REDE-SP)	Daily Maximum:	2
	SPIKE Minimum:	8,000
	SPIKE Maximum:	17,000
	Printed Pages:	10
	Folding:	Bifold

*REDE SPIKE: Represents the majority of the annual quantity for Mailers 5 and 6, which will transmit in one (1) session on the Monday before Labor Day in August of each year. Contractor must process, print, and mail the entire quantity within the timeframe specified in the contract production schedule (see "SCHEDULE" for additional information). NOTE: SSA anticipates an increase in the SCE notices at the time of the REDE SPIKE.

Mailer 7	Annual Minimum:	400,000
(CMS Letter 11198 and 11198-S)	Annual Maximum:	1,000,000
	Printed Pages:	12**
	Folding:	Bifold

NOTE: Mailer 7 files will transmit no later than the Friday after Labor Day each year. Exact quantities will not be known until live files are produced. An estimated quantity will not be provided each year prior to the actual live run. **Mailer 7 includes either the SSA-1020B-OCR-SM or SSA-1020B-OCR-SM-SP insert. This insert is included in the total number of printed pages.

Certified Mailers

Mailer 8	Daily Minimum:	0
(SSA-1020-OCR-SM or	Daily Maximum:	4
SSA-1020-OCR-SM-SP)	SPIKE Minimum:	10
	SPIKE Maximum:	25
	Printed Pages:	8
	Folding:	Bifold
Mailer 9	Daily Minimum:	0
(SSA-1026-OCR-SM-SCE or	Daily Maximum:	1
SSA-1026-OCR-SM-SCE-SP)	Printed Pages:	10
	Folding:	Bifold
Mailer 10	SPIKE Minimum:	100
(SSA-1026-OCR-SM-REDE or	SPIKE Maximum:	150
SSA-1026-OCR-SM-REDE-SP)	Printed Pages:	10
	Folding:	Bifold

NOTE: Mailers 8, 9, and 10 are the Certified Mail versions of Mailers 1 through 6, as follows: Mailer 8 is the Certified Mail version for Mailers 1 and 2; Mailer 9 is the Certified Mail version for Mailers 3 and 4; and Mailer 10 is the Certified Mail version for Mailers 5 and 6. Certified Mail is required for both English and Spanish versions.

CRITERIA FOR DATA IMAGING: At any point during the term of the contract, the Government reserves the right to move the data from record specific to AFP Fully Composed.

TRANSMISSIONS: Upon award of this contract, the Government will determine the connectivity method between SSA and the contractor. Internet Protocol (IP) will be the connection protocol for the transmissions.

The connectivity method will be through the Internet using an encrypted VPN tunnel, or the Government will place an order for a dedicated circuit data connection to be installed within 60 to 90 calendar days of award between the contractor's location and SSA's network interface location. Either connectivity method will be encrypted with the AES256 encryption algorithm. For the Internet option to be used, the contractor must have an Internet ready VPN IPSec capable hardware device. The Government will not be responsible for any cost associated with the VPN Internet connection that the contractor may incur. The connection method is at the sole discretion of the Government. The cost of the dedicated circuit connection will be borne by the Government. The Government shall not be responsible for installation delays of data connections due to any external influences such as employee strikes, weather, supplies, etc., which conditions are beyond the control of the Government.

If a dedicated circuit is deemed necessary, SSA will provide the dedicated data connection, including a router, and firewall at the contractor's specified locations. The contractor shall provide adequate rack space for securing the router and firewall; the contractor shall provide a dedicated analog dial-up line within eight (8) feet of the router. This dedicated analog dial-up line will be used for router management and access for troubleshooting. The line must be in place and active prior to the installation of the circuit/router and equipment.

Upon contract award, the contractor shall provide a complete delivery address with nearest cross-street, contact name, and phone number for installation of data transmission services and equipment. The contractor's contact person shall be available for delivery of services at the specified location. The Government shall not be responsible for incorrect or lack of address information nor for non-availability of contact person(s) at the delivery site.

It is the contractor's responsibility to notify SSA when systems or data line problems arise and transmission(s) cannot take place. SSA's first point of contact for systems or data line problems is the HELP DESK at (866) 718-6410. The contractor must call (866) 718-6410 and select Option 0 to establish a ticket. The contractor will describe the transmission issue to the help desk technician who will create a ticket number. After establishing a ticket, the print contractor must email the DBOPC.Leaders.Mailing.List@ssa.gov mailbox and include Melissa Picone at melissa.picone@ssa.gov on the email. The email must include the ticket number and identify any files that should have transmitted but did not, as well as a description of any other issues with the transmission.

Any reprogramming and/or reformatting of data supplied by wire transmission or VPN Internet transmission necessitated due to the contractor's method of production shall be the responsibility of the contractor and done at no cost to the Government.

FILE TRANSFER MANAGEMENT SYSTEM (FTMS) REQUIREMENTS: The contractor shall provide the capability to interface with SSA's National File Transfer Management System (FTMS) for electronic transmission of notice files from SSA to the production facility. SSA will provide the necessary data connection into the contractor's location. At the discretion of SSA, the line speed may be either increased or decreased depending on utilization. The contractor must provide, at their expense, the equipment and operating software platform and the file transfer software required at their location. The contractor assumes all responsibility for configuration, maintenance, and troubleshooting of their equipment and software.

SSA utilizes, and the contractor must provide compatibility with, file transfer technologies that SSA supports, which include SFTP and TIBCO Managed File Transfer software (MFT). The contractor may implement the Command Center Transfer Platform Server that has embedded software encryption capable of being enabled. If using TIBCO MFT, the personal computers/servers must have the capability to run Managed File Transfer software with encryption enabled using IP protocols on Windows, UNIX (i.e., IBM's AIX, SUN, or HP), or z/OS platforms.

SSA will not permit any private class A, B, or C IP addresses, (i.e., 10.xxx.xxx.xxx type IP addresses) from external users on its network. At connection time to SSA, the contractor will be provided a suitable IP address for access to SSA's network via a firewall. SSA will provide the necessary subnet(s) for connection at the remote site. The contractor will be responsible for their own name/address translation to fulfill the intended purpose of data transfers. SSA will exchange Managed File Transfer or SFTP configuration information with the contractor as required to accomplish file transfers.

The contractor may determine the media type on which files from SSA will be received, to the extent that operator intervention (e.g., a tape mount) is not required at SSA or the contractor's production facility. Simultaneous multiple transmission sessions must be possible on the contractor's equipment. All files transmitted by the SSA will be written as Physical Sequential or "flat" files at the contractor's location and will be distinguished with a "run date" in the contractor's file name.

Virtual Storage Access Method files and Generation Data Groups, supported by IBM/MVS or IBM z/OS operating systems, are not permitted under this contract. The contractor's storage format must not preclude the availability of the Managed File Transfer software Checkpoint/Restart feature.

NOTE: The contractor may not use VM/VSE/ESA on a mainframe system, as this hampers automated file transmission.

The contractor's FTMS software shall be operational for the receipt of data files 24 hours per day, seven (7) days per week, unless otherwise specified by the Government. The communications protocol between SSA and the contractor shall be the Internet Protocol. The contractor must specify the type of Local Area Network (LAN) connection that will be used at the location where the SSA connection is to be installed. The contractor is responsible for providing complete hardware and software compatibility with SSA's existing network. Production file transfers will be established according to SSA's standard procedures for transmission control, dataset naming, and resource security. The contractor's file management system must accommodate multiple file transmission sessions without intervention at either end. The contractor must have sufficient capacity to support the number of concurrent transmission file sessions as dictated by SSA.

The above will apply, regardless of the number of workloads transmitted to the contractor daily. If the contractor is awarded multiple SSA notice workloads, there must be sufficient capacity at the contractor's production facility to accept transmission of all files according to their schedules.

In the event that the transmission network is unavailable for a time period deemed critical by the Government, the files may, at the Government's option, be processed at the SSA print/mail facility.

It is the contractor's responsibility to notify SSA when systems or data line problems arise and transmission(s) cannot take place. SSA's first point of contact for systems or data line problems shall be the HELP DESK at (866) 718-6410. The contractor must call (866) 718-6410 and select Option 0 to establish a ticket. The contractor will describe the transmission issue to the help desk technician who will create a ticket number. After establishing a ticket, the print contractor must email the DBOPC.Leaders.Mailing.List@ssa.gov mailbox and include Melissa Picone at melissa.picone@ssa.gov on the email. The email must include the ticket number and describe the issue experienced (if files should have transmitted but did not, the email must include the file names of missing files).

NOTE: The contractor must not compress files.

All data provided by the Government or duplicates made by the contractor or their representatives and any resultant printouts must be accounted for and kept under strict security to prevent their release to any unauthorized persons.

Data may not be duplicated in whole or in part for any other purpose than to create material to be used in the performance of this contract.

Any duplicate data and any resultant printouts must be destroyed by the contractor. Data provided to the contractor must be retained for 21 workdays after mailing (before destruction).

FOR QUALITY CONTROL AND AUDITING PURPOSES: The contractor must not merge file dates and mailers during processing, printing, and mailing. All files transmitted by SSA will be physical sequential. Any alteration of the notice content in the file is not permitted.

PREPRODUCTION TESTS: Prior to the commencement of production of orders placed under this contract, the contractor will be required to demonstrate their ability to perform the contract requirements by performing the following tests –

- Transmission Test
- Preproduction Validation Test
- Construction Samples Validation Test
- Preproduction Press and Mail Run Test

The Government will furnish electronic test files at the postaward conference, or shortly thereafter, to be used in performing these tests.

The contractor must perform all Preproduction Tests in their facility and on their equipment using their personnel.

Failure by the contractor to perform any of the tests listed above to the satisfaction of the Government may be cause for default.

The Government reserves the right to waive the requirements of any or all of these tests. The contractor will be notified at the postaward conference, or shortly thereafter, if any test(s) will be waived.

The contractor will be required to have all material necessary to perform these tests. All composition and proofing must be completed prior to these tests, as applicable for each test (see "COMPOSITION" and "PROOFS" specified herein).

Government representatives will witness all phases of the Preproduction Press and Mail Run Test.

All PDF files containing PII must be sent via SFTP.

Whenever SSA initiates a systems/programming change, develops a new notice workload, or modifies an existing workload, the following test will be required before the notices go live:

- Systems Change/New and Existing Notice Files Validation Test.

Transmission Test: After the appropriate data connection has been installed, the contractor will be required to receive, within one (1) workday, data for approximately 650,000 notices (Mailers 1 through 10). These files will be sent concurrently, and the contractor will need to demonstrate their ability to receive them simultaneously.

The contractor will be required to perform a Record Count Verification and a Coding Accuracy Support System (CASS) certification within one (1) workday after the complete transmission of the test files.

The contractor will be required to copy the files to their own system and email Melissa Picone at melissa.picone@ssa.gov with the exact counts received (broken down by data set name), before proceeding with any other processing.

The contractor will be required to run the test files through their CASS certification system to ensure there are no problems with the reading of the address file. The contractor will be required to report to SSA with the test results.

SSA will respond within one (1) workday of receipt thereof.

Preproduction Validation Test: Within five (5) workdays of receipt of the Government's approval on all Scannable Forms, Worksheets, Letters, and Bulk Mailers 1BL and 2BL, the contractor must conduct a Preproduction Validation Test and furnish 656 printed samples (50* samples each of Mailers 1 through 6, Mailers 8 through 10, and Bulk Mailers 1BL and 2BL; and 53* samples each of Mailer 7 in both English and Spanish, one from each state.) for validation. Scannable Forms, Worksheets, and Letters must be complete and include all variable data from the Government-furnished test files and the PDF417 2D barcodes. Bulk Mailers 1BL and 2BL must be complete and include the PDF417 2D barcodes. No envelopes required.

Mailers 1, 2, and 8 (New Attainers) – The contractor must submit the printed samples as follows:

- 25 test samples for each mailer to: Social Security Administration, Wilkes-Barre Direct Operations Center, 1150 East Mountain Drive, Room 341, Wilkes-Barre, PA 18702-7997.

- 25 DUPLICATE test samples for each mailer* to: Social Security Administration, Attn: Melissa Picone, Printing and Postage, 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401. *NOTE: Press quality Adobe Acrobat PDF samples may be requested in addition to, or as an alternative to, printed samples for the Baltimore, MD address only.

The container and accompanying documentation for both locations must include the GPO Jacket, Purchase Order, Program, and Print Order Numbers.

Mailers 3, 4, 9 (SCE) and 5, 6, 10 (REDE) – The contractor must submit the printed samples as follows:

- 25 test samples for each mailer to: Social Security Administration, Wilkes-Barre Direct Operations Center, 1150 East Mountain Drive, Room 341, Wilkes-Barre, PA 18702-7997.

- 25 DUPLICATE test samples for each mailer* to: Social Security Administration, Attn: Melissa Picone, Printing and Postage, 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401. *NOTE: Press quality Adobe Acrobat PDF samples may be requested in addition to, or as an alternative to, printed samples for the Baltimore, MD address only.

The container and accompanying documentation for both locations must include the GPO Jacket, Purchase Order, Program, and Print Order Numbers.

Mailer 7 (CMS Letter) – The contractor must submit the printed samples as follows:

- 53 test samples each in both English and Spanish (one from each state)* to: Social Security Administration, Attn: Melissa Picone, Printing and Postage, 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401. *NOTE: Press quality Adobe Acrobat PDF samples may be requested in addition to, or as an alternative to, printed samples.

The container and accompanying documentation must include the GPO Jacket, Purchase Order, Program, and Print Order Numbers.

Bulk Mailers 1BL and 2BL – The contractor must submit the printed samples as follows:

- 25 test samples for each mailer to: Social Security Administration, Wilkes-Barre Direct Operations Center, 1150 East Mountain Drive, Room 341, Wilkes-Barre, PA 18702-7997.

- 25 DUPLICATE test samples for each mailer* to: Social Security Administration, Attn: Melissa Picone, Printing and Postage, 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401. *NOTE: Press quality Adobe Acrobat PDF samples may be requested in addition to, or as an alternative to, printed samples for the Baltimore, MD address only.

The container and accompanying documentation must include the GPO Jacket, Purchase Order, Program, and Print Order Numbers.

SSA will inspect all samples and test the samples with barcodes on their scanner and barcode reading device(s) as specified in these specifications.

The Government will approve, conditionally approve, or disapprove all preproduction validation samples within five (5) workdays of the receipt thereof. Approval or conditional approval shall not relieve the contractor from complying with the specifications and all other terms and conditions of the contract. A conditional approval shall state any further action required by the contractor. A notice of disapproval shall state the reasons thereof.

If contractor errors are found or author's alterations (AAs) are required, additional hard copy and/or PDF samples (as ordered) will be required within three (3) workdays of receipt of notification until such time as the validation produces no errors and no further AAs are needed.

The Government will approve, conditionally approve, or disapprove the additional preproduction validation samples within five (5) workdays of receipt thereof.

NOTE: The Government may require the contractor to make changes to the formats of the scannable forms, worksheets, letters, or envelopes at any time during the term of the contract. Whenever such copy changes are required, all aspects of the tests and "test schedules" must be maintained. Live production of all the mailers will continue during this transition period.

Construction Samples Validation Test: Within five (5) workdays of receipt of the Government's "O.K. to Print" on all the necessary components including the Preproduction Validation Test, the contractor must conduct a Construction Samples Validation Test and furnish 216 sample notice packages (10 samples each of Mailers 1 through 6, Mailers 8 through 10, and Bulk Mailers 1BL and 2BL; and 53 samples each of Mailer 7 in English and Spanish, one from each state) of the final completed product.

The samples must be complete and include all variable data from the Government-furnished test files and the PDF417 2D barcodes (except for Mailer 7, as it does not require a 2D barcode), inserted into the mail-out envelope with all required inserts and envelopes, leaving the mail-out envelope unsealed.

The contractor will be required to have all the necessary inserts and envelopes completed prior to beginning this validation test.

The contractor must send all test samples to: Social Security Administration, Attn: Melissa Picone, Printing and Postage, 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401. The container and accompanying documentation must include the GPO Jacket, Purchase Order, Program, and Print Order Numbers.

The Government will approve, conditionally approve, or disapprove the construction validation samples within five (5) workdays of the receipt thereof. Approval or conditional approval shall not relieve the contractor from complying with the specifications and all other terms and conditions of the contract. A conditional approval shall state any further action required by the contractor. A notice of disapproval shall state the reasons thereof.

If contractor errors are found, additional samples will be required within three (3) workdays of notification until such time as the validation produces no errors.

The Government will approve, conditionally approve, or disapprove the additional preproduction validation samples within three (3) workdays of receipt thereof.

Preproduction Press and Mail Run Test (12-Hour Test): Prior to commencement of production, the contractor will be required to demonstrate their ability to perform the contract requirements by performing a 12-hour Preproduction Press and Mail Run Test utilizing the test files transmitted electronically.

Within five (5) workdays of receipt of test files, final approval on the construction samples validation test, and the contractor's receipt of all necessary materials to perform the test (i.e., scannable forms, worksheets, letters, envelopes), the Government will work with the contractor to select a date when the contractor will be required to perform the 12-hour Preproduction Press and Mail Run Test.

The test shall occur during the regular workweek of Monday through Friday (excluding Federal holidays).

The Government will issue a print order for the Preproduction Press and Mail Run Test.

Upon successful completion of all test requirements, the contractor will be reimbursed for all applicable costs, in accordance with the contractor's submitted bid prices in the "SCHEDULE OF PRICES." If the contractor fails to meet all test requirements, they will not be reimbursed for any associated costs.

The contractor will be required to have all composition, proofing, envelopes, scanning equipment, and reports for 100% accountability of production and mailing completed, available, and ready for production prior to the beginning of the test. Notices are to be completed in accordance with contract requirements, inserted with applicable inserts into envelopes, and prepared for mailing.

Contractor will be required to provide the necessary audit and summary reports for 100% accountability of production and mailing within one (1) hour after the run is completed.

The contractor must produce a minimum of 99,221 notices, as follows from the transmission test, in a continuous 12-hour period that will prove to the Government representatives that the contractor can satisfactorily complete the requirements of this contract during live production:

Mailer 1	6,429
Mailer 2	571
Mailer 3	6
Mailer 4	1
Mailer 5	16,000
Mailer 6	1,214
Mailer 7	75,000
Total	99,221

The 12-hour period for the printing, inserting, and mailing process will begin when an "O.K. to Print" is given by the Government representative on site. The 12-hour period for the inserting, including any necessary reprints, and mailing process will begin within two (2) hours after the start of the printing to allow the contractor to print sufficient materials to begin the inserting process.

The test run will incorporate all aspects of the program consisting of the processing of electronically transmitted test files/data; the duplex printing and imaging of Mailers 1 through 7; personalized worksheet matched with scannable form; binding; construction; gathering; folding; inserting; reprints; manifesting; presorting; and preparing finished notices for delivery to the USPS. To simulate actual production conditions, the product produced must be in accordance with all contract specifications and all USPS regulations.

The contractor must perform the Preproduction Press and Mail Run Test on their equipment and using their personnel.

The test must be performed on the printing equipment and inserting machines with required scanning equipment that will be used in live production. All samples must be manufactured at the facility in which the contract production quantities are to be manufactured.

Samples of the preproduction press and mail run test will be brought back to SSA for validation.

The Government will approve, conditionally approve, or disapprove the validation output within seven (7) workdays of receipt thereof. Approval or conditional approval shall not relieve the contractor from complying with the specifications and all other terms and conditions of the contract. A conditional approval shall state any further action required by the contractor. A notice of disapproval shall state the reasons thereof.

Failure to meet the requirements of the 12-hour test is grounds to immediately terminate the contractor for default.

Systems Change/New and Existing Notice Files Validation Test: When required, the Government will furnish test files for transmission that are to be used in performing a Systems Change/New and Existing Notice Files Validation Test. This test is required whenever SSA initiates a systems/programming change, a new notice workload is developed, or an existing workload is changed.

NOTE: All workloads specified in this contract are updated annually including Bulk Forms 1BL and 2BL.

SSA may require press quality PDF and/or hard copy samples.

When required, the contractor must furnish PDF samples with variable data for each mailer, with each PDF sample containing a varying number of records from the test files, within three (3) workdays of receipt of the test files and/or approval of the PDF proofs without variable data, as applicable, via the SFTP site and email melissa.picone@ssa.gov once available. (NOTE: Quantity to be specified at time of test.)

When required, the contractor must furnish printed (hard copy) samples (no envelopes) with variable data for each mailer within three (3) workdays of receipt of the test files and/or approval of the PDF proofs with or without variable data, as applicable, to WBDOC for scanner testing. (NOTE: Quantity to be specified at time of test.)

The Government will approve, conditionally approve, or disapprove the samples within five (5) workdays of receipt thereof. Approval or conditional approval must not relieve the contractor from complying with the specifications and all other terms and conditions of the contract. A conditional approval must state any further action required by the contractor. A notice of disapproval must state the reasons thereof.

The test must occur without a break in production of notices. The Government will inform the contractor in advance when the test files are to be provided and what changes are taking place.

If errors are found, additional samples of notices (as indicated above) will be required until such time as the validation produces no errors.

Programming, PDFs, and printed (hard copy) samples shall be billed in accordance with the applicable line items in the “SCHEDULE OF PRICES.”

COMPOSITION: Typesetting for text and form work will be required as follows:

- Contractor will be required to typeset all scannable forms and worksheets utilizing Times New Roman, Arial, Script MT, Myriad Pro, and OCRA Std, OCRA Extended including bold and italic font styles.

- Contractor will be required to typeset the CMS Letter utilizing Times New Roman, Palatino, Helvetica, Arial, Arial Black, Malgun Gothic Bold, MS Gothic, Gulim, MS Mincho, and Symbol including bold and italic font styles.

- Contractor will be required to typeset all envelopes utilizing Helvetica, Arial, and Times including bold font styles.

No alternate typefaces will be allowed; however, manufacturers' generic equivalents will be accepted (upon Government approval) for the above typefaces.

SSA reserves the right to require samples and to judge the suitability of any equivalent typeface offered in order to make an award, which is deemed to be in the best interest of the Government.

NOTE: If required, the contractor must typeset the above from the furnished manuscript copy.

The entirety of each category of composition (text, tabular, and display) must be identical throughout the product(s)ordered under these specifications. Contractor is to match the type size on the manuscript copy. Exact spacing of scan boxes and variable data must be maintained for readability on pre-programmed scanning equipment.

Form work will be defined as matter set in all sizes and will include vertical, horizontal, and diagonal rules, box heads, numbered lines, checkboxes, arrows, type matter, etc., positioned in the proper location to provide spaces for information to be filled in individually.

PROOFS: Proofs will be required with the initial order and any time a copy change is required during the term of the contract. Proofs may be ordered without and with variable data.

Envelopes:

One (1) press quality Adobe Acrobat (most current version) PDF soft proof (for content only) using the same Raster Image Processor (RIP) that will be used to produce the final printed product. PDF proof will be evaluated for text flow, image position, and color breaks. Proof will not be used for color match.

For the envelopes, the PDF proofs must show all margins and dimensions, indicate trim marks, show flap, and window size and placement, as applicable.

***Scannable Forms, Worksheets, Letters, and Bulk Form 1BL and 2BL*:**

- One (1) press quality Adobe Acrobat (most current version) PDF soft proof (for content only) using the same Raster Image Processor (RIP) that will be used to produce the final printed product. PDF proof will be evaluated for text flow, image position, and color breaks. Proof will not be used for color match.

- Three (3) sets of digital color content proofs. Direct to plate must be used to produce the final product with a minimum resolution of 2400 x 2400 dpi. Proofs must be created using the same Raster Image Processor (RIP) that will be used to produce the product. Proofs must be collated with all elements in their proper position (not pasted up), imaged face and back, trimmed, and folded to the finished size as required for each item.

SSA reserves the right to make changes to all proofs. The Government may require one (1) or more sets of revised proofs before rendering an "O.K. to Print." Author's Alterations (AAs) may be required.

The contractor will be responsible for performing all necessary proofreading to ensure that the proofs are in conformity with the copy submitted.

If any contractor's errors are serious enough in the opinion of the GPO to require revised proofs, the revised proofs are to be provided at no additional expense to the Government. No extra time can be allowed for this reproofing operation; such operations must be accomplished within the original production schedule allotted in the specifications.

The contractor must not print prior to receipt of an "O.K. to Print."

PRIOR TO PRODUCTION SAMPLES (Envelopes Only): Samples of the envelopes may be required with the initial order and any time that a copy change may be required during the term of the contract.

When required, prior to the commencement of the contract production quantity, the contractor shall submit not less than two (2) samples of each envelope required on this contract (mail-out envelopes (window), mail-out envelopes (non-window), and the BRM return envelopes). The container and accompanying documentation shall be marked "PRIOR TO PRODUCTION SAMPLES" and shall include the GPO purchase order, jacket, program, and print order numbers.

All samples must be printed and constructed, as specified herein, and must be of the size, kind, and quality that the contractor will furnish. Samples will be inspected and tested for conformance of materials and must comply with the specifications as to construction, kind, and quality of materials. All samples must be printed on the required paper, as specified herein.

When required, the contractor must submit samples to: SSA, Attn: Melissa Picone, Printing and Postage, 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401.

Samples must be submitted within five (5) workdays of receipt of "O.K. to Print" on PDF proofs.

The Government will approve, conditionally approve, or disapprove the samples within two (2) workdays of the receipt thereof. Approval or conditional approval shall not relieve the contractor from complying with the specifications and all other terms and conditions of the contract. A conditional approval shall state any further action required by the contractor. A notice of disapproval shall state the reasons therefore.

If the samples are disapproved by the Government, the Government, at its option, may require the contractor to submit additional samples for inspection and test, in the time and under the terms and conditions specified in the notice of rejection. Such additional samples shall be furnished, and necessary changes made, at no additional cost to the Government. The Government will require the time specified above to inspect and test any additional samples required.

In the event that the samples are disapproved by the Government, the contractor shall be deemed to have failed to make delivery within the meaning of the default clause in which event this contract shall be subject to termination for default, provided however, that the failure of the Government to terminate the contract for default in such event shall not relieve the contractor of the responsibility to deliver the contract quantities in accordance with the shipping schedule.

In the event the Government fails to approve, conditionally approve, or disapprove the samples within the time specified, the Contracting Officer shall automatically extend the shipping schedule in accordance with article 12 "Notice of Compliance with Schedules" of contract clauses in GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987 (Rev. 01-18)).

Manufacture of the final product prior to approval of the samples submitted is at the contractor's risk. Samples will not be returned to the contractor. All costs, including the costs of all samples, shall be charged in accordance with the applicable pricing line item in the "SCHEDULE OF PRICES."

All samples shall be manufactured at the facilities and on the equipment in which the contract production quantities are to be manufactured.

STOCK/PAPER: The specifications of all paper furnished must be in accordance with those listed herein or listed for the corresponding JCP Code numbers in the "Government Paper Specification Standards No. 13" dated September 2019. Government Paper Specification Standards No. 13 - https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/vol_13.pdf.

Color of paper furnished shall be of a uniform shade and a close match by visual inspection of the JCP and/or attached color sample(s). The Contracting Officer reserves the right to reject shipments of any order printed on paper the color of which, in his or her opinion, materially differs from that of the color sample(s).

All paper used in each order must be of a uniform shade.

The contractor must furnish any required or requested samples on the specified stock.

Scannable Forms (Personalized and Non-Personalized) and Worksheets: White Optical Character Recognition (OCR) Bond, basis weight: 20 lbs. per 500 sheets, 17 x 22", equal to JCP Code O-25.

***CMS Letter**:* Uncoated Colored Text, basis weight: 50 lbs. per 500 sheets, 25 x 38", equal to JCP Code A63. NOTE: Stock must match International Paper, Springhill, Opaque Offset Gray for color and weight.

***BRM Return Envelopes**:* White Writing Envelope, basis weight: 20 lbs. per 500 sheets, 17 x 22", equal to JCP Code V20.

***Mail-out Envelopes**:* White Kraft Envelope, basis weight: 24 lbs. per 500 sheets, 17 x 22", equal to JCP Code V15; or, at contractor's option, White Uncoated Text, basis weight: 50 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60.

PRINTING AND IMAGING: All printing/imaging must have a minimum resolution of 600 x 600 dpi (see "Imaging" below). ***NOTE: Inkjet printing is not allowed.***

The Government reserves the right to make changes to the envelopes or to the format/text of the scannable forms, worksheets, or letters at any time during the term of the contract. Notification of a proposed change will be given with sufficient time for the contractor to allow for the change and submit proofs to the Government. The contractor is not to preprint or maintain more than a 90-calendar day surplus/inventory of any of the envelopes as required by this contract.

NOTE: The CMS Letter is an annual notice. All components required for the CMS Letter are excluded from the 90-calendar day surplus/inventory.

In the event that the agency makes changes to any or all of the envelopes, the Government will exhaust the current supply before requiring the contractor to begin using the updated components. The Government will not be required to purchase from the contractor the surplus/inventory of any stocked items remaining on-hand in excess of what was authorized when an envelope or format/text change is implemented. However, if a revision occurs which requires destruction of any stocked item, contractor will be allowed to charge for only those line items applicable in accordance with the "SCHEDULE OF PRICES."

Printing:

Scannable Forms (Personalized and Non-Personalized): Print face and back, head-to-head, in black ink only.

***Worksheets**:* Print face and back, head-to-head, in black ink only.

CMS Letters: Print face and back, head-to-head, in black ink only.

ALL Envelopes: Print face and back (after manufacturing) in black ink only. Printing must be in accordance with the requirements for the style envelope ordered. All printing must comply with all applicable U.S. Postal Service regulations. The envelope must accept printing without feathering or penetrating to the reverse side.

All envelopes require a security tint (straight-line tint is not acceptable) printed on the inside (back – before manufacturing) in black ink. The contractor may use their own design but must guarantee that the product will ensure complete opacity and prevent show through of any material contained therein. NOTE: The inside of the BRM return envelope must contain a clear area (no pantograph design) (approximate 3-1/2 x 5/8" in size), behind the IMb to ensure the readability by U.S. Postal Service equipment.

BRM Envelopes: Face of envelopes to be in BUSINESS REPLY FORMAT. Print the FIM and IMb using the furnished camera copy. Contractor is responsible for placing the FIM and IMb on the mail piece according to the current U.S. Postal Service Domestic Mail Manual.

Recycled Paper Logo and Legend:

See Government Paper Specification Standards No. 13 for recycled content requirements. If recycled paper is used, the recycled paper logo and legend must be printed in black ink as follows:

Scannable Forms (Personalized and Non-Personalized): The English recycled paper logo and legend must be printed on the first page of the English scannable forms in the lower left-hand corner. The Spanish recycled paper logo and legend must be printed on the first page of the Spanish scannable forms in the lower left-hand corner.

Worksheets*:* The English recycled paper logo and legend must be printed on the first page of the English worksheets in the lower left-hand corner. The Spanish recycled paper logo and legend must be printed on the first page of the Spanish worksheets in the lower left-hand corner.

Envelopes: The English recycled paper logo and legend must be printed on the back of all envelopes in the lower left-hand corner. If the envelope is bilingual, then the Spanish recycled paper logo and legend must also be printed on the back in the lower right-hand corner.

Imaging:

Contractor will be required to convert furnished data from the electronic transmission for laser/ion deposition printing in black ink with a minimum resolution of 600 x 600 dpi, utilizing Times New Roman, or equivalent serif typeface on the scannable forms and worksheets, and Arial Black and Time New Roman, or equivalent sans-serif and serif typeface on the CMS Letters in accordance with the following:

NOTE: Inkjet printing is not allowed.

Variable Data:

Scannable Forms SSA-1020-OCR-SM and SSA-1020-OCR-SM-SP

- *Face* – Up to six (6) lines of alphanumeric characters for the mailing address, plus the IMb.
- *Numbered Page 2* – Up to six (6) lines of alphanumeric characters in 12-point type, with one (1) character per box, subject to SSA approval.
- *Numbered Pages 2 through 7* – PDF417 2D barcode located at the top of each page.

Worksheets SSA-1026-OCR-SM-SCE, SSA-1020-OCR-SM-SCE-SP, SSA-1026-OCR-SM-REDE, and SSA-1026-OCR-SM-REDE-SP

- *Face* – Up to seven (7) lines of alphanumeric characters for the mailing address and applicant name, plus the IMb.
- *Back* – Up to 20 lines of alphanumeric characters in 12-point type, subject to SSA approval.

Scannable Forms SSA-1026-OCR-SM-SCE, SSA-1020-OCR-SM-SCE-SP, SSA-1026-OCR-SM-REDE, and SSA-1026-OCR-SM-REDE-SP

- *Numbered Page 2* – Up to six (6) lines of alphanumeric characters in 12-point type, with one (1) character per box, subject to SSA approval.
- *Numbered Pages 2 through 7* – PDF417 2D barcode located at the top of each page.

CMS Letter

- *Face* – Up to seven (7) lines of alphanumeric characters for the letter date and mailing address, plus the IMb.
- *Face to Back* - Up to five (5) lines of numeric and punctuation characters in the body of the notice.

NOTE: Bulk Mailers 1BL and 2BL **DO NOT** require computerized imaging of variable data. All Bulk Mailers must contain a PDF417 2D barcode at the top of numbered pages 2 through 7 of the form (see "BARCODE REQUIREMENTS" for additional information).

NOTE: Contractor is to produce a keyline that appears above the mailing address and shows through the window of the mail-out envelope. The keyline must contain the following information:

- Workload (1020, 1026 SCE, 1026 REDE)
- Mailer Number (M1E, M1R, M2S, M8C, M3E, M3R, M4S, M9C, M5E, M5R, M6S, M10C)
- File Date (yy/mm/dd)

Keyline Examples: 1020 M1E 261001; 1026 SCE M4E 260917; 1026 REDE M5S 260830.

BARCODE REQUIREMENTS: The scannable forms contain PDF417 (Portable Data File) 2D barcodes. Barcodes must not interfere with any wording on the forms.

The PDF417 2D barcodes must be in accordance with the requirements of ANSI MH 10.8.3M, unless otherwise specified. All data elements contained in the barcode must begin in the specified positions. Data elements can be filled with blanks if necessary to begin the next element in the proper position.

Data columns are to be preceded and followed by the standard PDF417 2D barcode stop/start patterns, left row indicator and right row indicator.

The PDF417 2D barcodes produced under these specifications must be guaranteed to function properly when scanned. The barcoding must be readable by all standard barcode scanning devices regardless of the contractor's method of reproducing the codes.

The data for the PDF417 2D barcodes on the personalized scannable forms will be contained in the SSA furnished data files. See the SSA furnished Vendor/Record Specifications for details.

PDF417 2D Barcode:

New Attainers: A PDF417 2D barcode will be required on all SSA-1020-OCR-SM and SSA-1020-OCR-SM-SP personalized scannable forms (top of numbered pages 2 through 7) as follows:

Located 1-1/8" from the left edge. At least 1/4" margins (quiet zone) is required top, bottom, left, and right of each PDF417 2D barcode. Height is 1/2", plus or minus 1/16"; length/width is 3-1/4", plus or minus 1/16". Maximum resolution of 300 dpi, with 4.41 code words per inch.

The PDF417 2D barcodes must contain the following data elements, as applicable:

Field Name	Field Size	
Form Number	20	
Page Number	2	(contractor to insert)
Vendor Name	4	
Applicant Last Name	20	

Applicant Suffix	4
Applicant First Name	15
Applicant Middle Initial	1
Applicant SSN	9
Spouse Last Name	20
Spouse Suffix	4
Spouse First Name	15
Spouse Middle Initial	1
Spouse SSN	9
Address Street 1	22
Address Street 2	22
Address City	19
Address State	2
Address Zip 1	5
Address Zip 2	4
Address Zip Delivery Point Code	3
Edition Date (Month)	2
Edition Date (Year)	4
Language Indicator	1
File Creation Date	8
Applicant Date of Birth	8
Spouse Date of Birth	8
Miscellaneous Data	18
Record Length	250

SCE and REDE: A PDF417 2D barcode will be required on all SSA-1026-OCR-SM-SCE, SSA-1026-OCR-SM-SCE-SP, SSA-1026-OCR-SM-REDE, and SSA-1026-OCR-SM-REDE-SP personalized scannable forms (top of numbered pages 2 through 7) as follows:

Located 1-1/8” from the left edge. At least 1/4” margins (quiet zone) is required top, bottom, left, and right of each PDF417 2D barcode. Height is 1/2”, plus or minus 1/16”; length/width is 3-1/4”, plus or minus 1/16”. Maximum resolution of 300 dpi, with 4.41 code words per inch.

The PDF417 2D barcodes must contain the following data elements, as applicable:

Field Name	Field Size	
Form Number	23	
Page Number	2	(contractor to insert)
Vendor Name	4	
Applicant Last Name	20	
Applicant Suffix	4	
Applicant First Name	15	
Applicant Middle Initial	1	
Applicant Date of Birth	8	
Applicant Medicare Claim Number	12	
Applicant SSN	9	
Spouse Last Name	20	
Spouse Suffix	4	
Spouse First Name	15	
Spouse Middle Initial	1	
Spouse Date of Birth	8	
Spouse Medicare Claim Number	12	

Spouse SSN	9
Address Street 1	22
Address Street 2	22
Address City	19
Address State	2
Address Zip 1	5
Address Zip 2	4
Address Zip Delivery Point Code	3
Edition Date (Month)	2
Edition Date (Year)	4
Language Indicator	1
File Creation Date	8
Miscellaneous Data	19
End of Record Indicator	1
Record Length	279

***Bulk Form 1BL and 2BL*:** A PDF417 2D barcode will be required on all SSA-1020B-OCR-SM and SSA-1020B-OCR-SM-SP non-personalized scannable forms (top of numbered pages 2 through 7) as follows:

Located 1-1/4" from the left edge. At least 1/4" margins (quiet zone) is required top, bottom, left, and right of each PDF417 2D barcode. Height is 3/8", plus or minus 1/16"; length/width is 1-1/8", plus or minus 1/16". Maximum resolution of 300 dpi, with 4.41 code words per inch.

The contractor will be required to perform the necessary programming to print the 2D barcodes on these scannable forms.

The PDF417 2D barcodes must be programmed to contain the following data elements:

Field Name	Field Size	
Form Number	20	
Page Number	2	
Language	1	(E for English, S for Spanish)
Edition Date (Month)	2	(MM)
Edition Date (Year)	4	(YYYY)
Vendor Name	4	

NOTE: Mailer 7 English uses the same bulk form (SSA-1020B-OCR-SM) as 1BL. Mailer 7 Spanish uses the same bulk form (SSA-1020B-OCR-SM-SP) as 2BL.

PRESS SHEET INSPECTION: Final makeready press sheets may be inspected and approved at the contractor's plant for the purpose of establishing specified standards for use during the actual press run. Upon approval of the sheets, contractor is charged with maintaining those standards throughout the press run (within QATAP tolerances when applicable) and with discarding all makeready sheets that preceded approval. See GPO Publication 315.3 (Guidelines for Contractors Holding Press Sheet Inspections) issued January 2015. NOTE: A press sheet inspection is for the purpose of setting specific standards that are to be maintained throughout the entire run. It does not constitute a prior approval of the entire run.

Viewing Light: Press sheets will be viewed under controlled conditions with 5000 degrees Kelvin overhead luminaries. The viewing conditions must conform to ISO 3664-2009. A viewing booth under controlled conditions with 5000 degrees Kelvin overhead luminaries with neutral gray surroundings must be provided.

NOTE: When a press sheet inspection is required, the Government will notify the contractor. A press sheet inspection(s) may be required at the contractor's/subcontractor's plant before production begins on any new or existing workload.

MARGINS: Contractor is to follow furnished manuscript copy, electronic file, or other given instructions for proper margins on the scannable forms, worksheets, letters, and envelopes.

BINDING:

Mailers 1, 2, and 8 (New Attainers):

Scannable Form (Personalized): Trim each 16-3/4 x 10-3/4" leaf four sides. Fold each 16-3/4 x 10-3/4" leaf down to 8-3/8 x 10-3/4", title out. The two folded 8-3/8 x 10-3/4" leaves are nested together to create an 8-page form.

Mailers 3, 4, 9 (SCE) and 5, 6, 10 (REDE):

Worksheet: Trim four sides.

Scannable Forms (Personalized): Trim each 16-3/4 x 10-3/4" leaf four sides. Fold each 16-3/4 x 10-3/4" leaf down to 8-3/8 x 10-3/4", title out. The two folded 8-3/8 x 10-3/4" leaves are nested together to create an 8-page form.

Mailer 7 (CMS Letter):

Letter: Trim four sides.

Scannable Form (Non-Personalized): Trim each 16-3/4 x 10-3/4" leaf four sides. Fold each 16-3/4 x 10-3/4" leaf down to 8-3/8 x 10-3/4", title out. The two folded 8-3/8 x 10-3/4" leaves are nested together to create an 8-page form.

Bulk Mailers 1BL and 2BL:

Scannable Form (Non-Personalized): Trim each 16-3/4 x 10-3/4" leaf four sides. Fold each 16-3/4 x 10-3/4" leaf down to 8-3/8 x 10-3/4", title out. The two folded 8-3/8 x 10-3/4" leaves are nested together to create an 8-page form.

CONSTRUCTION:

BRM Return Envelopes (5-3/4 x 8-3/4"): Envelopes must be open side with side seams and a gummed, fold-over flap for sealing. Flap depth is at contractor's option but must meet all USPS requirements. Flap must be coated with suitable glue the entire length of flap that will securely seal the return envelope for mailing. Adhesive must not adhere to the contents of the envelope.

Mail-out Envelopes (Window) for Mailers 1 through 10 (6-1/8 x 9-1/4"): Envelopes must be open side with side seams and a gummed, fold-over flap for sealing. Flap depth is at contractor's option but must meet all USPS requirements. Flap must be coated with a suitable glue that will securely seal the envelope without adhering to contents, permit easy opening by the recipient, and not permit resealing of the envelope. Mail-out envelopes to be securely sealed on all sides and must remain sealed under normal mailing conditions.

Face of envelope to contain one (1) die-cut address window (1-3/4 x 4-1/4" in size) with slightly rounded corners (the long dimension of the window is to be parallel to the long dimension of the envelope). Die-cut window is to be located 2" from the bottom edge and 3/4" from the left edge.

Contractor has the option to adjust the size of the window opening (subject to Government approval), providing the visibility of the computer generated mailing address and IMb on the notice is not obscured and other extraneous information is not visible when material is inserted into the envelope.

Windows are to be covered with a suitable transparent, low-gloss, poly-type, material that must be clear of smudges, lines, and distortions. Poly-type material must be securely affixed to the inside of the envelope so as not to interfere with insertion of contents. Window material must meet the current USPS readability standards/requirements. Address image must meet USPS reflectance standards when viewed through the window material.

Mail-out Envelopes (Non-Window) for Bulk Mailers 1BL and 2BL (6-1/8 x 9-1/4"): Envelopes must be open side with side seams and a gummed, fold-over flap for sealing. Flap depth is at contractor's option but must meet all USPS requirements. Flap must be coated with a suitable glue that will securely seal the envelope without adhering to contents, permit easy opening by the recipient, and not permit resealing of the envelope.

GATHERING AND INSERTING: Gather and fold (as specified below) for insertion into the mail-out envelope.

Mailers 1, 2, and 8 (New Attainers) – Each constructed mailer consists of three (3) components: (1) personalized scannable form, (2) BRM return envelope, and (3) mail-out envelope (window) into which components 1 and 2 are inserted for mailing.

- Fold the 8-page personalized scannable form from 8-3/8 x 10-3/4" down to 8-3/8 x 5-3/8", title out.
- Insert the personalized scannable form and the BRM return envelope, in that order, into the mail-out envelope. The recipient's name and address on the scannable form must be visible through the mail-out envelope window. Securely seal each mail-out envelope.

Mailers 3, 4, 9 (SCE) and 5, 6, 10 (REDE) – Each constructed mailer consists of four (4) components: (1) personalized worksheet, (2) personalized scannable form, (3) BRM return envelope, and (4) mail-out envelope (window) into which components 1 through 3 are inserted for mailing.

- Fold the personalized worksheet from flat size of 8-1/2 x 11" down to 8-1/2 x 5-1/2", title out.
- Fold the 8-page personalized scannable form from 8-3/8 x 10-3/4" down to 8-3/8 x 5-3/8", title out.
- Insert the personalized worksheet, the personalized scannable form, and the BRM return envelope, in that order, into the mail-out envelope. The recipient's name and address on the worksheet must be visible through the mail-out envelope window. Securely seal each mail-out envelope.

Mailer 7 (CMS Letter) – Each constructed mailer consists of four (4) components: (1) personalized letter, (2) non-personalized scannable form, (3) BRM return envelope, and (4) mail-out envelope (window) into which components 1 through 3 are inserted for mailing.

- Fold the 4-page personalized letter from flat size of 8-1/2 x 11" down to 8-1/2 x 5-1/2", title out.
- Fold the 8-page non-personalized scannable form from 8-3/8 x 10-3/4" down to 8-3/8 x 5-3/8", title out.
- Insert the personalized letter, the non-personalized scannable form, and the BRM return envelope, in that order, into the mail-out envelope. The recipient's name and address on the letter must be visible through the mail-out envelope window. Securely seal each mail-out envelope.

Bulk Mailers 1BL and 2BL – Each constructed bulk mailer consists of three (3) components: (1) non-personalized scannable form, (2) BRM return envelope, and (3) mail-out envelope (non-window) into which components 1 and 2 are inserted.

- Fold the 8-page non-personalized scannable form from 8-3/8 x 10-3/4" down to 8-3/8 x 5-3/8", title out.
- Insert the non-personalized scannable form and the BRM return envelope, in that order, into the non-window mail-out envelope. Do not seal envelope.

It is the contractor's responsibility to ensure that only the computer-generated address and Intelligent Mail barcode will be visible through the window of the mail-out envelope. The contractor must also ensure that the correct items for each mailing package are inserted and that only one copy of each required item (as applicable to each mailer) is inserted into the mail-out envelope.

In addition, it is the contractor's responsibility to ensure that the personalized worksheet with recipient's name and other personal information is matched with the scannable form (containing 2D barcode with personalized data) for the same recipient before inserting into the mail-out envelope.

PACKING (Bulk Shipment Mailers 1BL and 2BL): Shrink-wrap completed bulk mailers in units of 25 or 50 (contractor's option). Pack suitable in shipping containers not to exceed 45 pounds when fully packed. Packing must not cause bowing of product.

All shipments which fill less than a shipping container must be packaged with materials of sufficient strength and durability and in such a manner which will guarantee that the product will not be damaged, and the package will not open or split when shipping.

Pallets are required.

LABELING AND MARKING (Bulk Shipment Mailers 1BL and 2 BL): Contractor to download the "Labeling and Marking Specifications" form (GPO Form 905, R. 7-15) from gpo.gov, fill in appropriate blanks, and attach to shipping containers.

Barcode Markings: Labels must be barcoded on shipping containers, using Uniform Symbology Specifications - Code 39 (new standard) barcode system, for non-contact reading, in accordance with ANSI/AIM BCI-1995. The barcode must be positioned in accordance with Fed. Std. 123.

Barcode Requirement: The barcode must be a 3 of 9 barcode, with an x-dimension of 10 millimeters. The barcode must have a human-readable interpretation (HRI) printed above or below the 3 of 9 barcode. The barcode information must include the following:

- Product ID (SSA-1020B-OCR-SM or SSA-1020B-OCR-SM-SP)
- Quantity per Container
- Unit of Issue
- Revision Date
- Requisition Number
- GPO Jacket Number
- Print Order Number

The destination address in the "TO" box does not have to be filled in on the individual shipping container labels when packed on pallets. In lieu thereof, complete filled in labels, including the destination address, must be attached to all four sides of each pallet. In addition to regular markings, include all items listed above.

PRODUCTION INSPECTION: Production inspection(s) may be required at the contractor's/subcontractor's plant for the purpose of establishing that the receipt of transmitted files; the printing of notices/forms and/or envelopes; and the imaging, collating, folding, gathering, inserting, packing, and mailing are being accomplished in accordance with contract quality attributes and requirements.

A production inspection is for the purpose of setting specific standards that are to be maintained throughout the entire run. It does not constitute a prior approval of the entire run. A production inspection(s) may be required at the contractor's/subcontractor's plant before production begins on any new workload.

When a production inspection is required, the Government will notify the contractor.

DISTRIBUTION:

- Deliver f.o.b. destination (on the first order and whenever SSA makes a significant change to the language, format, or appearance of a notice/form) 10 complete sample mailers of each notice/form type (along with any required insert(s)) inserted into mail-out envelopes. (DO NOT SEAL ENVELOPES.) Samples must be delivered to Social Security Administration, Attn: Melissa Picone, Printing and Postage, 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401.

- Deliver f.o.b. destination (on the first order and whenever SSA makes a copy change to any envelope) 10 printed samples of each envelope to: Social Security Administration, Attn: Melissa Picone, Printing and Postage, 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401.

- Deliver f.o.b. destination all required quality control samples to: Social Security Administration, Attn: Melissa Picone, Printing and Postage, 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401.

- Mail f.o.b. contractor's city each individual mailer. (The contractor is responsible for all costs incurred in transporting the mailers to the U.S. Postal Service facility.)

- Deliver f.o.b. destination the Bulk Mailers 1BL and 2BL via Small Package Common Carrier (SPCC) (499 pounds or less) or Reimbursable Freight (500 pounds or more) to the multiple locations specified on the print order. All f.o.b. destination shipments/bulk mailers must ship as a full truckload/complete in accordance with local prevailing times on normal Government workdays).

Small Package Common Carrier – Third-Party Billing:

Packages weighing up to and including 499 pounds are to be made by SPCC except those destined for Post Office Boxes, APO/FPO, and United States Possessions and Territories.

The Social Security Administration will provide the name and account number for the SPCC. When used, the contractor will be responsible for providing the carrier with the following:

1. All packages addressed and sorted to meet the requirements of the small package common carrier. NOTE: Contractor may be required to apply special SPCC barcode labels.

2. Separate common carrier pickup records for each print order. The contractor must annotate the pickup records with the requisition number and the print order number.

3. A shipping manifest which includes:

   (a) The name of the contractor, the requisition number, the print order number, and the common carrier account/shipper number.

(b) A listing which includes each addressee's account number or office code (when provided on SSA supplied address labels), address, city, state, zip code, common carrier delivery zone, weight, and package identification number (if applicable) of each package shipped to each addressee.

(c) The listing must be grouped by pickup, and each group must be identified with the pickup record number. This number must correspond to the number on the form(s) which the contractor is required to obtain from the carrier for compliance purposes. The listing must be in either account number or ZIP code order within each group.

(d) The summary information for each group must include the total number of packages, the total weight, and the total shipping cost.

The contractor will be required to ship via SPCC charging the cost to SSA's Third-Party account number, which will be provided after award.

Reimbursable Freight:

A single shipment to one address weighing 500 pounds or more is to be shipped by reimbursable freight. The contractor will be responsible for selection of carrier and must ship by the most reasonable method to ensure prompt delivery and safe arrival at all destinations for shipments requiring Commercial Bills of Lading.

All costs are to be billed on the contractor's invoices at the actual cost which the contractor paid for these services. Shipments must be made direct to the destination(s) stated on the print order.

Unless otherwise indicated, truck deliveries must be made at the point of destination between the hours of 8:30 a.m. and 3:00 p.m., local prevailing time, on standard Government workdays. Shipments must be delivered as specified.

Domestic First-Class Letter-Size Mail: The contractor is required to prepare domestic First-Class letter-size mail in accordance with appropriate USPS rules and regulations, including the USPS Domestic Mail Manual and Postal Bulletins in effect at the time of the mailing.

SSA requires the use of Seamless Acceptance. Seamless Acceptance is a USPS program automating the entry and verification of Full-Service mailings using electronic documentation (eDoc) and Intelligent Mail Barcodes.

Under Seamless Acceptance, the USPS does not require mailings of less than 200 pieces or 50 pounds to be metered.

SSA requires the use of Permit Imprint. The contractor must use SSA's "Postage and Fees Paid First Class Mail" permit imprint mailing indicia printed on each mail piece. Each mail piece sent under this payment method must bear a permit imprint showing that postage is paid. Permit imprint indicia may be printed directly on mail pieces.

The contractor is cautioned to use the permit imprint only for mailing material produced under this contract.

The contractor is required to obtain the maximum USPS postage discounts possible in accordance with the USPS First-Class Domestic Mail automated and nonautomated mail discount structure in effect at the time of mailing: (a) Automation (5-digit); (b) Automation (AADC); (c) Automation (Mixed AADC); (d) Nonautomation (Presorted); and (e) Nonautomation (Single Piece).

Mail addressed to United States possessions (e.g., American Samoa, Federated States of Micronesia, Guam, Marshall Islands, Northern Mariana Islands, Palau, Puerto Rico, U.S. Virgin Islands, and Wake Island) and Military Overseas Addresses (APO/FPO mail) is Domestic Mail, not International Mail, and should be included in the discount sorting above.

To maximize automation discounts, Intelligent Mail Barcode (IMb) barcoding, delivery address placement and envelopes used for the mailing are among the items that must comply with USPS requirements for automation-compatible mail in effect at the time of the mailing.

Contractor will be required to produce and use a USPS Intelligent Mail Barcode Full-Service option and achieve the maximum postage discounts available with this option. The contractor will be required to comply with USPS requirements and place the IMb on all mail pieces of this contract workload. The contractor is required to be capable of achieving the postage discounts available with the Full-Service option of the IMb program. The Full-Service option requires the contractor to use Postal One.

SSA will provide the contractor with a 6-digit Mailer Identifier (MID) for the mailing. The Mailer Identifier (MID) is a field within the Intelligent Mail Barcode that is used to identify the owner of the mail.

USPS has instituted a verification procedure called a "tap" test. This test is used to screen all mailings with barcoded inserts for proper barcode spacing within the envelope window. When the insert showing through the window is moved to any of its limits inside the envelope, the entire barcode must remain within the barcode clear zone. In addition, a clear space must be maintained that is at least 0.125 (1/8) inch between the barcode and the left and right edges of the window and at least 0.028-inch clearance between the Intelligent Mail Barcode and the top and bottom edges of the window.

All letters in a mailing must pass the "tap" test in order to obtain the maximum postal discounts for the agency. The contractor will be responsible for payment of any additional postage resulting from a loss of postage discounts due to failure to pass the "tap" test because of inaccuracy or failure to conform to USPS specifications

USPS Certified Mail: During the term of this contract, the contractor will be required to mail Certified Mailers 8, 9, and 10 in accordance with the USPS regulations contained in the Domestic Mail Manual (DMM) under section 503.3.0, Certified Mail. Notices associated with the certified mail file shall be inserted into envelopes and processed as certified mail. The contractor must place the current U.S. Postal Service 20-digit certified number and barcode on the envelope. The contractor must prepare the file as a separate permit imprint mailing of identical weight pieces using the appropriate U.S. Postal Service mailing statement.

International First-Class Mail: International Mail is not required on this contract. See "REQUEST FOR FOREIGN NOTICE PULLS FROM FILE PRIOR TO PRODUCTION." However, if, at any point during the term of the contract, International First-Class Mail is required, or if a new workload is added that requires International First-Class Mail, the contractor must mail in accordance with these specifications.

All items mailed must conform to the appropriate USPS International Mail Manual, Postal Bulletins, and other USPS rules and regulations in effect at the time of mailing.

Permit Imprint is to be used for SSA International Mail.

If the mailing meets the qualifications for International Priority Airmail (IPA), it must be processed through IPA in accordance with USPS rules and regulations in effect at the time of the mailing. Contractor must prepare mail pieces in accordance with the shape-based requirements of First-Class Mail International service listed in the USPS International Mail Manual and the additional requirements for IPA as specified in the most recent IMM. The contractor is required to sort the mail to achieve the maximum postage discounts available with the IPA program. To maximize postage savings, the contractor shall sort to the IPA Rate Group 1 through 15. Due to heightened security, many foreign postal administrations require complete sender and addressee information in roman letters and arabic numerals on postal items.

The complete address of the sender, including ZIP Code and country of origin, should be shown in the upper left corner of the address side of the envelope.

International Mail return addresses must show as the last line of the address "UNITED STATES OF AMERICA," or "USA," all in upper-case letters. All International Mail must be endorsed "PAR AVION" or "AIR MAIL," as described in the USPS IMM. The contractor may use a rubber stamp to meet these requirements.

NOTE: International mail cannot contain a presort endorsement. Again, mail addressed to United States possessions (e.g., American Samoa, Federated States of Micronesia, Guam, Marshall Islands, Northern Mariana Islands, Palua, Puerto Rico, U.S. Virgin Islands and Wake Island), and Military Overseas addresses (APO/FPO mail) is Domestic Mail, NOT International Mail.

***National Change of Address (NCOA) and Coding Accuracy Support System (CASS*):** The files provided by SSA to the contractor may or may not be CASS or NCOA certified. Contractor will be required to complete all necessary processing to obtain certification and mail discounts for USPS.

The contractor shall run all addresses through NCOA and CASS software for address accuracy. The contractor cannot change the addresses, but if an address fails CASS or NCOA or requires a NCOA move update, the contractor shall sort those pieces into a separate file and mail at the non-automated presort rate or full postage rate as to avoid any USPS fines for failure to meet address accuracy rules imposed by USPS. If contractor fails to meet this requirement, the Government will not reimburse for any USPS imposed fines. All related costs to perform this operation must be included in submitted bid pricing. No additional reimbursement will be authorized.

IMPORTANT: Contractor CANNOT at any time perform move updates or address corrections on the notice address. Notices that require a move update can be separated/diverted and sent at the full USPS first class rate. If the contractor uses a mail sort house, the furnished mail package must not receive an updated mailing address label.

Certificate of Conformance: GPO Form 712 – Certificate of Conformance (Rev. 10-15). A fillable GPO Form 712 Certificate of Conformance can be found at https://www.gpo.gov/how-to-work-with-us/vendors/forms-and-standards.

Mailing Documentation: The contractor must provide SSA with complete copies of all documents used by USPS to verify and accept the mail (e.g., computer records of presort ZIP+4, barcode breakdown, press runs, etc.) including USPS 3607R and/or GPO's Form 712 (Certificate of Conformance) and/or Certificate of Bulk mailing, etc. Each document must be noted with file date and mailer number.

The contractor must place the number that is on top of the GPO Form 712 (the number that starts with "A") in the space provided on the USPS mailing statements. If no space is provided on the mailing statement, place the number in the upper right margin of the mailing statement. The contractor will also use SSA's Federal Agency Cost Code **276-00070** on all mailing documents for Mailers 1, 2, 3, 4, 5, 6, 8, 9, and 10 and SSA's Federal Agency Cost Code **271-09800** on all mailing documents for Mailer 7 which must be placed on all mailing documents. All copies must be legible and include both obverse and reverse side.

Mailing Documentation and Summary Reports: A PDF copy of the summary report(s) and matching USPS Certificate of Bulk Mailing, USPS 3607R, and/or GPO 712 form(s) must be submitted to melissa.picone@ssa.gov for each file date within two (2) workdays of mailing. All copies must be legible and include both obverse and reverse side.

Invoices: Within three (3) workdays following the completion of each print order, the contractor must submit via email one (1) copy of the contractor's billing invoice showing amount of billing invoice to melissa.picone@ssa.gov. The original invoice will be sent to the U.S. Government Publishing Office. (See "PAYMENT.")

Quality Control Samples: Each container of quality control samples must contain the samples for a particular print order in a separate container. The contractor must ship the quality control samples each week within two (2) workdays following the final mailing date of the print order.

Upon completion of this contract, the contractor must email PDF files (current version) of all base forms, worksheets, letter, and envelopes to Melissa Picone at melissa.picone@ssa.gov.

All expenses incidental to picking up and returning materials (as applicable), submitting and picking up proofs (as applicable), construction samples from the validation test, prior to production samples, and furnishing sample copies must be borne by the contractor.

SCHEDULE: Adherence to this schedule must be maintained. Contractor must not start production of any job prior to receipt of the electronic daily counts and/or print order (GPO Form 2511), as applicable. If the contractor does not receive the electronic daily counts, they must notify SSA by email at: melissa.picone@ssa.gov.

In the event that it becomes necessary for the contractor to deviate from the specified mail-out date or the quantity to be mailed, SSA must be notified immediately.

If applicable, manuscript copy, camera copy, PDF file, or electronic media for forms, worksheets, letters, and envelopes will be provided at the postaward conference, or shortly thereafter.

When required, hard copy proofs must be delivered to and picked up from: Social Security Administration, Attn: Melissa Picone, Printing and Postage, 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401.

If applicable, furnished manuscript/camera copy must be returned with hard copy proofs.

When required, contractor to email PDF proofs as instructed by SSA.

Proof Schedule:

The following schedules begin the workday after receipt of furnished materials; the workday after receipt will be the first workday of the schedule.

NOTE: Hard copy proofs will not be returned to the contractor.

Envelopes:

- Contractor to submit all required PDF proofs within seven (7) workdays of receipt of furnished materials.
- Proofs will be withheld no more than five (5) workdays from receipt at the ordering agency until receipt of corrections/changes/"O.K. to Print" via email. (NOTE: The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.)
- If AAs are required, contractor to submit revised PDF proofs within three (3) workdays of notification until such time as no further AAs are needed.
- Revised proofs will be withheld no more than three (3) workdays from receipt at the ordering agency until receipt of corrections/changes/"O.K. to Print" via email. (NOTE: The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.)

Scannable Forms, Worksheets, and Letters:

Without Variable Data –

- Contractor to submit all required PDF proofs for ***initial proofs*** within 21 workdays of receipt of furnished materials and for ***other than initial proofs*** within five (5) workdays of receipt of furnished materials.

- Proofs will be withheld no more than five (5) workdays from receipt at the ordering agency until receipt of corrections/changes/"O.K. to Print" via email. (NOTE: The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.)

- If AAs are required, contractor to submit revised PDF proofs within three (3) workdays of notification until such time as no further AAs are needed.

- Revised proofs will be withheld no more than five (5) workdays from receipt at the ordering agency until receipt of corrections/changes/"O.K. to Print" via email. (NOTE: The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.)

With Variable Data (other than live production) –

- Contractor to submit all required PDF proofs with variable data within three (3) workdays of receipt of proof approval on PDF proofs without variable data.

- Proofs will be withheld no more than five (5) workdays from receipt at the ordering agency until receipt of corrections/changes/"O.K. to Print" via email. (NOTE: The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.)

- Contractor to submit all required hard copy proofs with variable data within three (3) workdays of receipt of proof approval on PDF proofs with variable data.

- Proofs will be withheld no more than five (5) workdays from receipt at the ordering agency until receipt of corrections/changes/"O.K. to Print" via email. (NOTE: The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.)

- If AAs are required, contractor to submit revised PDF and/or hard copy proofs, as ordered, within three (3) workdays of notification until such time as no further AAs are needed.

- Revised proofs will be withheld no more than five (5) workdays from receipt at the ordering agency until receipt of corrections/changes/"O.K. to Print" via email. (NOTE: The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.)

Live Production –

- Contractor to submit all required PDF and/or hard copy proofs for the scannable forms, worksheets, and letters within one (1) workday of receipt of the live production files.

- Proofs will be withheld no more than two (2) workdays from receipt at the ordering agency until receipt of corrections/changes/"O.K. to Print" via email for PDF and/or hard copy proofs. (NOTE: The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.)

- If AAs are required, contractor to submit revised PDF and/or hard copy proofs, as ordered, within one (1) workday of notification until such time as the proofs produce no errors and no further AAs are needed.

- Revised proofs will be withheld no more than two (2) workdays from receipt at the ordering agency until receipt of corrections/changes/"O.K. to Print" via email for PDF and/or hard copy proofs.

***Bulk Form 1BL and 2BL*:** Bulk Mailers 1BL and 2BL **DO NOT** require computerized imaging of variable data. All Bulk Mailers must contain a PDF417 2D barcode at the top of numbered pages 2 through 7 of the form (see "BARCODE REQUIREMENTS" for additional information).

- Contractor to submit all required PDF proofs for ***initial proofs*** within 21 workdays of receipt of furnished materials and for ***other than initial proofs*** within five (5) workdays of receipt of furnished materials.

- Proofs will be withheld no more than five (5) workdays from receipt at the ordering agency until receipt of corrections/changes/"O.K. to Print" via email. (NOTE: The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.)

- Contractor to submit all required hard copy proofs within three (3) workdays of receipt of proof approval on PDF proofs.

- Proofs will be withheld no more than five (5) workdays from receipt at the ordering agency until receipt of corrections/changes/"O.K. to Print" via email. (NOTE: The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.)

- If AAs are required, contractor to submit revised PDF and/or hard copy proofs, as ordered, within three (3) workdays of notification until such time as no further AAs are needed.

- Revised proofs will be withheld no more than five (5) workdays from receipt at the ordering agency until receipt of corrections/changes/"O.K. to Print" via email. (NOTE: The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.)

Preproduction Test Schedules:

Transmission Test:

- The contractor will be required to receive approximately 650,000 notices (Mailers 1 through 10) within one (1) workday.

- The contractor will be required to perform a Record Count Verification and CASS certification within one (1) workday after the complete transmission of the test files.

- SSA will verify that the counts match and notify the contractor within one (1) workday.

Preproduction Validation Test:

- Within five (5) workdays of receipt of the Government's approval on all Scannable Forms, Worksheets, Letters, and Bulk Mailers 1BL and 2BL, the contractor must conduct a Preproduction Validation Test and furnish 656 printed samples (50 samples each of Mailers 1 through 6, Mailers 8 through 10, and Bulk Mailers 1BL and 2BL; 53 samples each of Mailer 7 in both English and Spanish, one from each state) for validation.

- The Government will approve, conditionally approve, or disapprove the preproduction validation samples within five (5) workdays of the receipt thereof.

- If contractor errors are found or AAs are required, additional samples will be required within three (3) workdays of receipt of notification until such time as the validation produces no errors and no further AAs are needed.

- The Government will approve, conditionally approve, or disapprove the additional preproduction validation samples within five (5) workdays of receipt thereof.

Construction Samples Validation Test:

- Within five (5) workdays of receipt of the Government's "O.K. to Print" on all the necessary components including the Preproduction Validation Test, the contractor must conduct a Construction Samples Validation Test and furnish 216 sample notice packages (10 samples each of Mailers 1 through 6, Mailers 8 through 10, and Bulk Mailers 1BL and 2BL; 53 samples each of Mailer 7 in English and Spanish, one from each state) of the final completed product.

- The Government will approve, conditionally approve, or disapprove the construction validation samples within five (5) workdays of the receipt thereof.

- If contractor errors are found, additional samples will be required within three (3) workdays of notification until such time as the validation produces no errors.

- The Government will approve, conditionally approve, or disapprove the additional preproduction validation samples within three (3) workdays of receipt thereof.

Preproduction Press and Mail Run Test (12-Hour Test):

- Within five (5) workdays of receipt of test files, final approval on the construction samples validation test, and the contractors receipt of all necessary materials to perform the test (i.e., scannable forms, worksheets, letters, envelopes), the Government will work with the contractor to select a date when the contractor will be required to perform the 12-hour Preproduction Press and Mail Run Test.

- The contractor must produce a minimum of 99,221 notices in a continuous 12-hour period.

- The Government will approve, conditionally approve, or disapprove the validation output within seven (7) workdays of receipt thereof.

Systems Change/New and Existing Notice Files Validation Test:

- When required, the contractor must furnish PDF samples with variable data for each mailer, with each PDF sample containing a varying number of records from the test files, within three (3) workdays of receipt of the test files and/or approval of the PDF proofs without variable data, as applicable.

- When required, the contractor will furnish printed (hard copy) samples (no envelopes) with variable data for each mailer within three (3) workdays of receipt of the test files and/or approval of the PDF proofs with or without variable data, as applicable.

- The Government will approve, conditionally approve, or disapprove the samples within five (5) workdays of receipt thereof.

Production Schedule:

Workday - The term "workday" is defined as Monday through Friday* each week, exclusive of the days on which Federal Government holidays are observed.

Federal Government Holidays are as follows: New Year's Day, Martin Luther King's Birthday, President's Day, Memorial Day, Juneteenth Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day, and Christmas Day.

*NOTE: The contractor's FTMS software shall be operational for the receipt of data files 24 hours a day, seven (7) days a week, unless otherwise specified by the Government. (See "FILE TRANSFER MANAGEMENT SYSTEM (FTMS) REQUIREMENTS" for additional information).

Daily Medicare Notices (Mailers 1, 2, 3, 4, 5, 6, 8, 9, and 10): Production files will transmit daily Monday through Saturday.

New Attainers SPIKE (Mailers 1, 2, and 8): Production files will transmit between the 24th and 28th of each month.

REDE SPIKE (Mailers 5, 6, and 10): Production files will transmit in one (1) session on the Monday before Labor Day in August of each year. The REDE SPIKE represents the majority of the annual Redetermination quantity. Subsequent quantities will be minimal to none.

CMS Letter (Mailer 7): Production files will transmit in one (1) session no later than the Friday after Labor Day in September of each year.

Bulk Mailer Requirement: Approximately one (1) or two (2) print orders will be issued each year for Bulk Mailers 1BL and 2BL. One order will be placed in December, and, if required, a second order may be placed around mid-year.

The following schedules begin the workday after notification of availability of the electronic notice counts and furnished materials; the workday after notification will be the first workday of the schedule.

Contractor must complete production and mailing of all Medicare Notice mailers in accordance with the following schedule:

New Attainers (Mailers 1, 2, and 8) – Complete production and mailing must be made within five (5) workdays after receipt of each complete transmission.

New Attainers SPIKE (Mailers 1, 2, and 8) – Complete production and mailing must be made within seven (7) workdays after receipt of each complete transmission.

SCE (Mailers 3, 4, and 9) and REDE (5 ,6, and 10) – Complete production and mailing must be made within seven (7) workdays after receipt of each complete transmission.

REDE Spike (Mailers 5, 6, and 10) – Complete production and mailing must be made within seven (7) workdays after receipt of each complete transmission. Contractor must provide daily production reports via email to melissa.picone@ssa.gov for the REDE SPIKE notice run.

CMS Letter (Mailer 7) – Complete production and mailing must be made over a maximum of 10 workdays starting the third Monday in September of each year. Contractor will be required to mail a minimum of 100,000 notices per day until completed. Contractor must provide daily production reports via email to melissa.picone@ssa.gov for the CMS Letter notice run.

Bulk Mailer Shipment (1BL and 2BL) – Complete production and distribution must be made within ten (10) workdays after receipt of the print order for orders up to and including 350,000 copies. Contractor will be allowed one (1) additional workday for each additional 150,000 copies, or portion thereof.

PRESS SHEET AND PRODUCTION INSPECTIONS: The contractor must notify the GPO of the date and time that the press sheet or production inspection can be performed. In order for proper arrangements to be made, notification must be given at least seven (7) workdays prior to the inspection(s). Notify the U.S. Government Publishing Office, Quality Control for Published Products, Washington, DC 20401 at (202) 512-0542 AND Melissa Picone via email at melissa.picone@ssa.gov. Telephone calls to GPO will only be accepted between the hours of

8:00 a.m. and 2:00 p.m., prevailing Eastern Time, Monday through Friday. NOTE: See contract clauses, paragraph 14(e) (1), Inspections and Tests in GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987 (Rev. 01-18)). When supplies are not ready at the time specified by the contractor for inspection, the Contracting Officer may charge to the contractor the additional cost of the inspection.

NOTE: If the backup facility is used for the production of these notices, the Government will require a press sheet inspection. Prior to production in that facility, notification must be given at least seven (7) workdays in advance of production startup.

The ship/deliver date indicated on the print order is the date products ordered for delivery f.o.b. destination must be delivered to the destination(s) specified and the date products ordered for mailing f.o.b. contractor's city must be delivered to the U.S. Postal Service.

Unscheduled material such as shipping documents, receipts or instructions, delivery lists, and labels will be furnished with the order or shortly thereafter. In the event such information is not received in due time, the contractor will not be relieved of any responsibility in meeting the shipping schedule because of failure to request such information..

For compliance reporting purposes, the contractor must notify the U.S. Government Publishing Office of the date of shipment or delivery, as applicable. Upon completion of each order, contractor must contact the Shared Support Services Compliance Section via email at compliance@gpo.gov; or via telephone at (202) 512-0520. Personnel receiving the email or call will be unable to respond to questions of a technical nature or to transfer any inquiries.

SECTION 3. – DETERMINATION OF AWARD

The Government will determine the lowest bid by applying the prices offered in the "SCHEDULE OF PRICES" to the following units of production, which are the estimated requirements to produce one (1) year's production under this contract. These units do not constitute, nor are they to be construed as, a guarantee of the volume of work which may be ordered under this contract for a like period of time.

The following item designations correspond to those listed in the "SCHEDULE OF PRICES."

I.	(a)	12
	(b)	4
II.	(a)	80
	(b)	18
III.	(a)	1
	(b)	1
	(c)	1
	(d)	1
IV.	(a)	18
	(b)	14
	(c)	38
	(d)	240
	(e)	1
V.	(a)	250
	(b)	7,604
	(c)	2,232
	(d)	3,802
	(e)	3,452
	(f)	350
VI.	(a)	7,604
	(b)	232
	(c)	2,000
	(d)	3,802
	(e)	3,452
	(f)	350
VII.	(a)	3,452
	(b)	350
	(c)	375
VIII.		505
IX.		1

THIS PAGE IS INTENTIONALY BLANK.

SECTION 4. – SCHEDULE OF PRICES

Bids offered are f.o.b. contractor's city for all mailing and f.o.b. destination for all other consignments.

Prices must include the cost of all required materials and operations for each item listed in accordance with these specifications.

Bidder must make an entry in each of the spaces provided. Bids submitted with any obliteration, revision, or alteration of the order and manner of submitting bids may be declared non-responsive.

An entry of NC (No Charge) shall be entered if bidder intends to furnish individual items at no charge to the Government. Bids submitted with NB (No Bid), NA (Not Applicable), or blank spaces for an item may be declared non- responsive.

The Contracting Officer reserves the right to reject any offer that contains prices for individual items of production (whether or not such items are included in the "DETERMINATION OF AWARD") that are inconsistent or unrealistic in regard to other prices in the same offer or to GPO prices for the same operation if such action would be in the best interest of the Government.

All billing invoices submitted to the GPO shall be based on the most economical method of production. Fractional parts of 1,000 will be prorated at the per-1,000 rate.

Contractor's billing invoice must be itemized in accordance with the line items in the "SCHEDULE OF PRICES."

Cost of all required paper must be charged under Item VI. "PAPER."

I. PROCESSING/FORMATTING FILES AND SUBSEQUENT PROGRAMMING: The contractor will be allowed only one (1) charge per mailer for the term of the contract to process and/or format the files supplied necessary to print and mail the notices for each notice workload. Subsequent programming may be required if SSA initiates a systems/programming change, develops a new notice workload, or modifies an existing workload.

(a) Processing/Formatting files ..... per mailer ..... $ _____

(b) Subsequent Programming..... per hour ..... $ _____

II. COMPOSITION: Prices offered must include the cost of all materials and operations necessary for the complete composition of the products listed in accordance with these specifications.

Any change in the format on any page or on any envelope will be charged under line item (a) or (b), as applicable. For line item II.(a), a charge will be allowed for each 8-3/8 x 10-3/4" or 8-1/2 x 11" page, as applicable.

(a) Notices: Scannable Forms (per 8-3/8 x 10-3/4" page),
Worksheets and CMS Letters (per 8-1/2 x 11" page) ..... per page ..... $ _____

(b) Envelopes ..... per envelope ..... $ _____

_____
(Initials)

III. PREPRODUCTION TESTS: Price offered must include all costs incurred in performing the preproduction tests as specified in these specifications. These costs shall cover but are not limited to: machine time, personnel, all required materials, transmissions, electronic prepress, plates, paper, printing, imaging, collating, inserting, mail preparation, and any other operations necessary to produce the required quantities of the products in the time specified and in accordance with specifications.

(a) Transmission Test ..... per test .....$ _____

(b) Preproduction Validation Test ..... per test .....$ _____

(c) Construction Samples Validation Test ..... per test .....$ _____

(d) Preproduction Press and Mail Run Test ..... per test .....$ _____

IV. PROOFS AND PRIOR TO PRODUCTION SAMPLES:

(a) PDF Soft Proof: Envelopes ..... per proof .....$ _____

(b) PDF Soft Proof: Notices *(without variable data)* -
Scannable Forms, Worksheets, and CMS Letters ..... per proof .....$ _____

(c) PDF Soft Proof: Notices (*with variable data)* -
Scannable Forms, Worksheets, and CMS Letters ..... per test/live file .....$ _____

(d) Digital Color Content Proof*:* Notices -
Scannable Forms (per 8-3/8 x 10-3/4" page),
Worksheets and CMS Letters (per 8-1/2 x 11" page) ..... per page ..... $ _____

(e) Prior to Production Samples: Envelopes ..... per order .....$ _____

V. PRINTING, IMAGING, BINDING, AND CONSTRUCTION: Prices offered must be all-inclusive and must include the cost of all required materials and operations (excluding paper and proofs) necessary for the printing, imaging, binding, and construction of the products listed in accordance with these specifications.

(a) *Daily Makeready/setup charge ..... _____$

*Contractor will be allowed only one (1) makeready/setup charge per workday. This combined charge shall include all materials and operations necessary to makeready and/or setup the contractor's equipment. Invoices submitted with more than one makeready/setup charge per workday will be disallowed.

(b) Scannable Forms (16-3/4 x 10-3/4" flat) ..... per 1,000 leaves .....$ _____

(c) Worksheets and CMS Letters (8-1/2 x 11") ..... per 1,000 leaves .....$ _____

(d) BRM Return Envelopes..... per 1,000 envelopes .....$ _____

(e) Mail-out Envelopes (Window) ..... per 1,000 envelopes .....$ _____

(f) Mail-out Envelopes (Non-Window)..... per 1,000 envelopes .....$ _____

_____
(Initials)

VI. PAPER: Payment for all paper supplied by the contractor under the terms of these specifications, as ordered on the individual print orders, will be based on the net number of leaves furnished for the product(s) ordered. The cost of any paper required for makeready or running spoilage must be included in the prices offered.

Computation of the net number of leaves will be based on the following:

Scannable Forms (16-3/4 x 10-3/4"): A charge will be allowed for each page-size leaf.
Worksheets and CMS Letters (8-1/2 x 11"): A charge will be allowed for each page-size leaf.
ALL Envelopes – One leaf will be allowed for each envelope.

Per 1,000 Leaves

(a) Scannable Forms: White OCR Bond (20-lb.)..... $ _____

(b) Worksheets: White OCR Bond (20-lb.) ..... $ _____

(c) CMS Letters: Opaque Offset Gray Uncoated Colored Text (50-lb.)..... $ _____

(d) BRM Return Envelopes: White Writing (20-lb.) ..... $ _____

(e) Mail-out Envelopes (Window): White Kraft Envelope (24-lb.);
or, at contractor's option, White Uncoated Text (50-lb.) ..... $ _____

(f) Mail-out Envelopes (Non-Window): White Kraft Envelope (24-lb.);
or, at contractor's option, White Uncoated Text (50-lb.) ..... $ _____

VII. GATHERING, INSERTING, PACKING, AND MAILING: Prices offered must include the cost of all required materials and operations necessary for the mailing of the notice(s) (including cost of gathering (single or multiple leaves) in proper sequence, collating all required items (as specified) in proper sequence, and folding to required size in accordance with these specifications for insertion into mail-out envelopes; insertion of all appropriate items, as required, into appropriate mail-out envelope); packing and shipping of the Bulk Mailers 1BL and 2BL (including the cost of packing; shipping containers; pallets; all necessary wrapping and packing materials; labeling and marking); and, distribution in accordance with these specifications.

(a) Mailers 1 through 10 ..... per 1,000 mailers .....$ _____

(b) Bulk Mailers 1BL and 2BL ..... per 1,000 mailers .....$ _____

(c) Bulk Mailers 1BL and 2BL:
Packing and sealing shipping containers ..... per container .....$ _____

_____
(Initials)

VIII. CERTIFIED/REGISTERED MAIL: Prices offered must include the cost of any and all additional materials (i.e., paper, envelopes, printing, labels, etc.) and operations necessary to complete the Certified/Registered mail and provide to the USPS. This price is in addition to the "SCHEDULE OF PRICES" for Items I. through VII. listed above.

Certified/Registered Mail ..... per mailer .....$ _____

IX. ADDITIONAL OPERATIONS:

Destruction of Stocked Items.....per 1,000 pieces .....$ _____

_____
(Initials)

SHIPMENTS: Shipments will be made from: City _____ State _____ .

The city(ies) indicated above will be used for evaluation of transportation charges when shipment f.o.b. contractor's city is specified. If no shipping point is indicated above, it will be deemed that the bidder has selected the city and state shown below in the address block, and the bid will be evaluated and the contract awarded on that basis. If shipment is not made from evaluation point, the contractor will be responsible for any additional shipping costs incurred.

DISCOUNTS: Discounts are offered for payment as follows: _____ Percent _____ Calendar Days. See Article 12 "Discounts" of Solicitations Provisions in GPO Contract Terms (Publication 310.2).

AMENDMENT(S): Bidder hereby acknowledges amendment(s) number(ed) _____ .

BID ACCEPTANCE PERIOD: In compliance with the above, the undersigned agree, if this bid is accepted within _____ calendar days (90 calendar days unless a different period is inserted by the bidder) from the date for receipt of bids, to furnish the specified items at the price set opposite each item, delivered at the designated point(s), in exact accordance with specifications. *NOTE: Failure to provide a 90-day bid acceptance period may result in expiration of the bid prior to award.*

BIDDER'S NAME AND SIGNATURE: Unless specific written exception is taken, the bidder, by signing and submitting a bid, agrees with and accepts responsibility for all certificate ions and representations as required by the solicitation and GPO Contract Terms – Publication 310.2. When responding by email, fill out and return one copy of all pages in "SECTION 4. – SCHEDULE OF PRICES," including initialing/signing where indicated. Valid electronic signatures will be accepted in accordance with the Uniform Electronic Transactions Act, §2. Electronic signatures must be verifiable of the person authorized by the company to sign bids. *Failure to sign the signature block below may result in the bid being declared non-responsive.*

Bidder _____
(Contractor's Name) (GPO Contractor's Code)

_____
(Street Address)

_____
(City – State – Zip Code)

By _____
(Signature and Title of Person Authorized to Sign this Bid) (Date)

_____
(Printed Name) (Telephone Number)

_____
(Email) (Fax Number)

THIS SECTION FOR GPO USE ONLY

Certified by: _____ Date: _____ Contracting Officer: _____ Date: _____
(Initials) (Initials)

EXHIBIT A

CONTRACTOR PERSONNEL SECURITY CERTIFICATION

Purpose: This form is used for contractor personnel to certify that they understand SSA's security and confidentiality requirements.

I understand the SSA security and confidentiality requirements and agree that:

1. I will follow all SSA rules of conduct and security policy/privacy rules/regulations.

2. I agree not to construct and maintain, for a period of time longer than required by the contract, any file containing SSA data unless explicitly agreed to by SSA in writing as part of the task documentation.

3. I agree to safeguard SSA information, whether electronic or hardcopy, in secured and locked containers during transportation.

4. I will use all computer software according to Federal copyright laws and licensing agreements.

5. I agree to keep confidential any third-party proprietary information which may be entrusted to me as part of the contract.

6. I will comply with systems security requirements contained in the SSA Systems Security Handbook.

7. I will not release or disclose any information subject to the Privacy Act of 1974, the Tax Return Act of 1976, SSA Regulation 1 and section 1106 of the Social Security Act to any unauthorized person.

8. I understand that disclosure of any information to parties not authorized by SSA may lead to criminal prosecution under Federal law.

---	---
Contractor	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date

----------	----------
Contractor Employee	Date
----------	----------
Contractor Employee	Date
----------	----------
Contractor Employee	Date
----------	----------
Contractor Employee	Date
----------	----------
Contractor Employee	Date
----------	----------
Contractor Employee	Date
----------	----------
Contractor Employee	Date
----------	----------
Contractor Employee	Date
----------	----------
Contractor Employee	Date
----------	----------
Contractor Employee	Date
----------	----------
Contractor Employee	Date
----------	----------
Contractor Employee	Date

---	---
Contractor Employee	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date
---	---
Contractor Employee	Date

EXHIBIT B

1. SYSTEM IDENTIFICATION

1.1. System Name/Title: [State the name of the system. Spell out acronyms.]

1.1.1. System Categorization: Moderate Impact for Confidentiality

1.1.2. System Unique Identifier: [Insert the System Unique Identifier]

1.2. Responsible Organization:

Name:	
Address:	
Phone:	

1.2.1. Information Owner - Government point of contact responsible for providing and/or receiving Controlled Unclassified Information (CUI)**:**

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.2.1.1. System Owner (assignment of security responsibility)**:**

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.2.1.2. System Security Officer:

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.3. General Description/Purpose of System: What is the function/purpose of the system? **[Provide a short, high-level description of the function/purpose of the system.]**

1.3.1. Number of end users and privileged users: **[In the table below, provide the *approximate* number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, etc. Add rows to define different roles as needed.]**

Roles of Users and Number of Each Type:

Number of Users	Number of Administrators/ Privileged Users

1.4. General Description of Information: Controlled Unclassified Information (CUI) information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at https://www.archives.gov/cui/registry/category-list. [**Document the CUI information types processed, stored, or transmitted by the system below**].

2. SYSTEM ENVIRONMENT

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note**:** *this does not require depicting every workstation or desktop*, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram.
[Insert a system topology graphic. Provide a narrative consistent with the graphic that clearly lists and describes each system component.]

2.1. Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component. **[Insert the reference/URL or note that the hardware component inventory is attached.]**

2.2. List all software components installed on the system. **[Insert the reference/URL or note that the software component inventory is attached.]**

2.3. Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization? **[Yes/No - If no, explain:]**

3. REQUIREMENTS

(Note: The source of the requirements is NIST Special Publication 800-171, dated December 2016)

Provide a thorough description of how all of the security requirements are being implemented or planned to be implemented. The description for each security requirement contains: 1) the security requirement number and description; 2) how the security requirement is being implemented or planned to be implemented; and 3) any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the requirement is not applicable to the system, provide rationale.

3.1. Access Control

3.1.1. Account Management

a. Define the types of system accounts allowed and prohibited.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Create, enable, modify, disable, and remove system accounts in accordance with policy, procedures, prerequisites, and criteria.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Specify:

1. Authorized users of the system,
2. Group and role membership, and
3. Access authorizations (i.e., privileges) for each account.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Authorize access to the system based on:

1. A valid access authorization and
2. Intended system usage.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

e. Monitor the use of system accounts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

f. Disable system accounts when:

1. The accounts have expired,
2. The accounts have been inactive for [Assignment: organization-defined time period],
3. The accounts are no longer associated with a user or individual,
4. The accounts are in violation of organizational policy, or
5. Significant risks associated with individuals are discovered.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

g. Notify account managers and designated personnel or roles within:

1. [Assignment: organization-defined time period] when accounts are no longer required.

2. [Assignment: organization-defined time period] when users are terminated or transferred.
3. [Assignment: organization-defined time period] when system usage or the need-to-know changes for an individual.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

h. Require that users log out of the system after [Assignment: organization-defined time period] of expected inactivity or when [Assignment: organization-defined circumstances].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.2. Access Enforcement:

Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.3. Information Flow Enforcement

Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.4. Separation of Duties

a. Identify the duties of individuals requiring separation.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Define system access authorizations to support separation of duties of individuals to reduce the risk of malevolent activity without collusion.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.5. Least Privilege

a. Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Authorize access to [Assignment: organization-defined security functions] and [Assignment: organization-defined security-relevant information].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Review the privileges assigned to roles or classes of users [Assignment: organization-defined frequency] to validate the need for such privileges.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Reassign or remove privileges, as necessary.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.6. Least Privilege – Privileged Accounts

a. Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Require that users (or roles) with privileged accounts use non-privileged accounts when accessing non-security functions or non-security information.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.7. Least Privilege – Privileged Functions

a. Prevent non-privileged users from executing privileged functions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Log the execution of privileged functions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.8. Unsuccessful Logon Attempts

a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action] when the maximum number of unsuccessful attempts is exceeded.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.9. System Use Notification

Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting access to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.10. Device Lock

a. Prevent access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.11. Session Termination

Terminate a user session automatically after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.12. Remote Access

a. Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Authorize each type of remote system access prior to establishing such connections.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Route remote access to the system through authorized and managed access control points.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Authorize the remote execution of privileged commands and remote access to security-relevant information.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.13. Withdrawn

Incorporated into 03.01.12.

3.1.14. Withdrawn

Incorporated into 03.01.12.

3.1.15. Withdrawn

Incorporated into 03.01.12.

3.1.16. Wireless Access

a. Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Authorize each type of wireless access to the system prior to establishing such connections.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Disable, when not intended for use, wireless networking capabilities prior to issuance and deployment.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Protect wireless access to the system using authentication and encryption.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.17. Withdrawn
Incorporated into 03.01.16.

3.1.18. Access Control for Mobile Devices

a. Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Authorize the connection of mobile devices to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Implement full-device or container-based encryption to protect the confidentiality of CUI on mobile devices.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.19. Withdrawn
Incorporated into 03.01.18.

3.1.20. Use of External Systems

a. Prohibit the use of external systems unless the systems are specifically authorized.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after:

1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and

2. Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.21. Withdrawn

Incorporated into 03.01.20.

3.1.22. Publicly Accessible Content

a. Train authorized individuals to ensure that publicly accessible information does not contain CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review the content on publicly accessible systems for CUI and remove such information, if discovered.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.2. Awareness and Training

3.2.1. Literacy Training and Awareness

a. Provide security literacy training to system users:
   1. As part of initial training for new users and [Assignment: organization- defined frequency] thereafter,
   2. When required by system changes or following [Assignment: organization- defined events], and
   3. On recognizing and reporting indicators of insider threat, social engineering, and social mining.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.2.2. Role-Based Training

a. Provide role-based security training to organizational personnel:
   1. Before authorizing access to the system or CUI, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter.
   2. When required by system changes or following [Assignment: organization-defined events].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.2.3. Withdrawn

Incorporated into 03.02 01.

3.3. Audit and Accountability

3.3.1. Event Logging

a. Specify the following event types selected for logging within the system: [Assignment: organization-defined event types].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update the event types selected for logging [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.2. Audit Record Content

a. Include the following content in audit records:
   1. What type of event occurred
   2. When the event occurred
   3. Where the event occurred
   4. Source of the event

5. Outcome of the event
6. Identity of the individuals, subjects, objects, or entities associated with the event.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Provide additional information for audit records as needed.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.3. Audit Record Generation

a. Generate audit records for the selected event types and audit record content specified in **03.03.01** and **03.03.02**.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Retain audit records for a time period consistent with the records retention policy.Review and update logged events.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.4. Response to Audit Logging Process Failures

a. Alert organizational personnel or roles within [Assignment: organization-defined time period] in the event of an audit logging process failure.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Take the following additional actions: [Assignment: organization-defined additional actions].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.5. Audit Record Review, Analysis, and Reporting

a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications and the potential impact of inappropriate or unusual activity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Report findings to organizational personnel or roles.
Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.6. Audit Record Reduction and Report Generation

a. Implement an audit record reduction and report generation capability that supports audit record review, analysis, reporting requirements, and after-the-fact investigations of incidents.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Preserve the original content and time ordering of audit records.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.7. Time Stamps

a. Use internal system clocks to generate time stamps for audit records.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.8. Protection of Audit Information

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Authorize access to management of audit logging functionality to only a subset of privileged users or roles.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.9. Withdrawn

Incorporated into 03.03.08.

3.4. Configuration Management

3.4.1. Baseline Configuration

a. Develop and maintain under configuration control, a current baseline configuration of the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update the baseline configuration of the system [Assignment: organization-defined frequency] and when system components are installed or modified.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.2. Configuration Settings

a. Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Identify, document, and approve any deviations from established configuration settings.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.3. Configuration Change Control

a. Define the types of changes to the system that are configuration controlled.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security impacts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Implement and document approved configuration-controlled changes to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Monitor and review activities associated with configuration-controlled changes to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.4. Impact Analyses

a. Analyze changes to the system to determine potential security impacts prior to change implementation.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Verify that the security requirements for the system continue to be satisfied after the system changes have been implemented.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.5. Access Restrictions for Change

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.6. Least Functionality

a. Configure the system to provide only mission-essential capabilities.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Prohibit or restrict use of the following functions, ports, protocols, connections, and services: [Assignment: organization-defined functions, ports, protocols, connections, and services].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Review the system [Assignment: organization-defined frequency] to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.7. Withdrawn

Incorporated into 03.04.06 and 03.04.08.

3.4.8. Authorized Software – Allow by Exception

a. Identify software programs authorized to execute on the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Implement a deny-all, allow-by-exception policy for the execution of authorized software programs on the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Review and update the list of authorized software programs [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.9. Withdrawn

Addressed by 03.01.05, 03.01.06, 03.01.07, 03.04.08, and 03.12.03.

3.4.10. System Component Inventory

a. Develop and document an inventory of system components.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update the system component inventory [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Update the system component inventory as part of installations, removals, and system updates.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.11. Information Location

a. Identify and document the location of CUI and the system components on which the information is processed and stored.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Document changes to the system or system component location where CUI is processed and stored.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.12. System and Component Configuration for High-Risk Areas

a. Issue systems or system components with the following configurations to individuals traveling to high-risk locations: [Assignment: organization-defined system configurations].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Apply the following security requirements to the systems or components when the individuals return from travel: [Assignment: organization-defined security requirements].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5. Identification and Authentication

3.5.1. User Identification, Authentication, and Re-Authentication.

a. Uniquely identify and authenticate system users and associate that unique identification with processes acting on behalf of those users.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Re-authenticate users when [Assignment: organization-defined circumstances or situations requiring re-authentication].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.2. Device Identification and Authentication
Uniquely identify and authenticate [Assignment: organization-defined devices or types of devices] before establishing a system connection.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.3. Multi-Factor Authentication
Implement multi-factor authentication for access to privileged and non-privileged accounts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.4. Replay-Resistant Authentication
Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.5. Identifier Management

a. Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Select and assign an identifier that identifies an individual, group, role, service, or device.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Prevent the reuse of identifiers for [Assignment: organization-defined time period].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.6. Withdrawn

Consistency with SP 800-53.

3.5.7. Password Management

a. Maintain a list of commonly used, expected, or compromised passwords, and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Transmit passwords only over cryptographically protected channels.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Store passwords in a cryptographically protected form.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

e. Select a new password upon first use after account recovery.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

f. Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.8. Withdrawn
Consistency with SP 800-53.

3.5.9. Withdrawn
Consistency with SP 800-53.

3.5.10. Withdrawn
Incorporated into 03.05.07.

3.5.11. Authentication Feedback
Obscure feedback of authentication information during the authentication process.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.12. Authenticator Management
a. Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Establish initial authenticator content for any authenticators issued by the organization.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Change default authenticators at first use.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

f. Protect authenticator content from unauthorized disclosure and modification.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6. Incident Response

3.6.1. Incident Handling

Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6.2. Incident Monitoring, Reporting, and Response Assistance

a. Track and document system security incidents.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Report incident information to [Assignment: organization-defined authorities].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Provide an incident response support resource that offers advice and assistance to system users on handling and reporting incidents.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6.3. Incident Response Testing

Test the effectiveness of the incident response capability [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6.4. Incident Response Training

a. Provide incident response training to system users consistent with assigned roles and responsibilities:
   1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access,
   2. When required by system changes, and
   3. [Assignment: organization-defined frequency] thereafter.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6.5. Incident Response Plan

a. Develop an incident response plan that:
   1. Provides the organization with a roadmap for implementing its incident response capability,
   2. Describes the structure and organization of the incident response capability,
   3. Provides a high-level approach for how the incident response capability fits into the overall organization,
   4. Defines reportable incidents,
   5. Addresses the sharing of incident information, and
   6. Designates responsibilities to organizational entities, personnel, or roles.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Distribute copies of the incident response plan to designated incident response personnel (identified by name and/or by role) and organizational elements.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Protect the incident response plan from unauthorized disclosure.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7. Maintenance

3.7.1. Withdrawn

Recategorized as NCO.

3.7.2. Withdrawn

Incorporated into 03.07.04 and 03.07.06.

3.7.3. Withdrawn

Incorporated into 03.08.03.

3.7.4. Maintenance Tools

a. Approve, control, and monitor the use of system maintenance tools.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Check media with diagnostic and test programs for malicious code before it is used in the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Prevent the removal of system maintenance equipment containing CUI by verifying that there is no CUI on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.5. Nonlocal Maintenance

a. Approve and monitor nonlocal maintenance and diagnostic activities.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Implement multi-factor authentication and replay resistance in the establishment of nonlocal maintenance and diagnostic sessions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Terminate session and network connections when nonlocal maintenance is completed.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.6. Maintenance Personnel

a. Establish a process for maintenance personnel authorization.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Maintain a list of authorized maintenance organizations or personnel.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8. Media Protection

3.8.1. Media Storage

Physically control and securely store system media that contain CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.2. Media Access

Restrict access to CUI on system media to authorized personnel or roles.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.3. Media Sanitization

Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.4. Media Marking

Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.5. Media Transport

a. Protect and control system media that contain CUI during transport outside of controlled areas.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Maintain accountability of system media that contain CUI during transport outside of controlled areas.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Document activities associated with the transport of system media that contain CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.6. Withdrawn

Addressed by 03.13.08.

3.8.7. Media Use

a. Restrict or prohibit the use of [Assignment: organization-defined types of system media].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Prohibit the use of removable system media without an identifiable owner.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.8. Withdrawn
Incorporated into 03.08.07.

3.8.9. System Backup – Cryptographic Protection
a. Protect the confidentiality of backup information.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI at backup storage locations.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.9. Personnel Security

3.9.1. Personnel Screening
a. This Screen individuals prior to authorizing access to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.9.2. Personnel Termination and Transfer

a. When individual employment is terminated:
   1. Disable system access within [Assignment: organization-defined time period],
   2. Terminate or revoke authenticators and credentials associated with the individual, and
   3. Retrieve security-related system property.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. When individuals are reassigned or transferred to other positions in the organization:
   1. Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility, and
   2. Modify access authorization to correspond with any changes in operational need.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10. Physical Protection

3.10.1. Physical Access Authorizations

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Issue authorization credentials for facility access.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Review the facility access list [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Remove individuals from the facility access list when access is no longer required..

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.2. Monitoring Physical Access

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.3. Withdrawn

Incorporated into 03.10.07.

3.10.4. Withdrawn

Incorporated into 03.10.07.

3.10.5. Withdrawn

Incorporated into 03.10.07.

3.10.6. Alternate Work Site

a. Determine alternate work sites allowed for use by employees.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Employ the following security requirements at alternate work sites: [Assignment: organization-defined security requirements].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.7. Physical Access Control

a. Enforce physical access authorizations at entry and exit points to the facility where the system resides by:
   1. Verifying individual physical access authorizations before granting access to the facility and
   2. Controlling ingress and egress with physical access control systems, devices, or guards.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Maintain physical access audit logs for entry or exit points.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Escort visitors, and control visitor activity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Secure keys, combinations, and other physical access devices.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

e. Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.8. Access Control for Transmission

Control physical access to system distribution and transmission lines within organizational facilities.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.11. Risk Assessment

3.11.1. Risk Assessment

a. Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Update risk assessments [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.11.2. Vulnerability Monitoring and Scanning

a. Monitor and scan the system for vulnerabilities [Assignment: organization-defined frequency] and when new vulnerabilities affecting the system are identified.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Remediate system vulnerabilities within [Assignment: organization-defined response times].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Update system vulnerabilities to be scanned [Assignment: organization-defined frequency] and when new vulnerabilities are identified and reported.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.11.3. Withdrawn

Incorporated into 03.11.02.

3.11.4. Risk Response

Respond to findings from security assessments, monitoring, and audits.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12. Security Assessment

3.12.1. Security Assessment

Assess the security requirements for the system and its environment of operation [Assignment: organization-defined frequency] to determine if the requirements have been satisfied.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.2. Plan of Action and Milestones

a. Develop a plan of action and milestones for the system:
   1. To document the planned remediation actions to correct weaknesses or deficiencies noted during security assessments and
   2. To reduce or eliminate known system vulnerabilities.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Update the existing plan of action and milestones based on the findings from:
   1. Security assessments,
   2. Audits or reviews, and
   3. Continuous monitoring activities.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.4. Withdrawn
Incorporated into 03.15.02.

3.12.5. Information Exchange

a. Approve and manage the exchange of CUI between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements; other types of agreements].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Document interface characteristics, security requirements, and responsibilities for each system as part of the exchange agreements.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Review and update the exchange agreements [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13. System and Communications Protection

3.13.1. Boundary Protection

a. Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Connect to external systems only through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.2. Withdrawn
Recategorized as NCO.

3.13.3. Withdrawn
Addressed by 03.01.01, 03.01.02, 03.01.03, 03.01.04, 03.01.05, 03.01.06, and 03.01.07.

3.13.4. Information in Shared System Resources
Prevent unauthorized and unintended information transfer via shared system resources.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.5. Withdrawn
Incorporated into 03.13.01.

3.13.6. Network Communications – Deny by Default – Allow by Exception
Deny network communications traffic by default and allow network communications traffic by exception.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.7. Withdrawn
Addressed by 03.01.12, 03.04.02 and 03.04.06.

3.13.8. Transmission and Storage Confidentiality

Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.9. Network Disconnect

Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.10. Cryptographic Key Establishment and Management

Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.11. Cryptographic Protection

Implement the following types of cryptography to protect the confidentiality of CUI: [Assignment: organization-defined types of cryptography].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.12. Collaborative Computing Devices and Applications

a. Prohibit the remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Provide an explicit indication of use to users physically present at the devices.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.13. Mobile Code

a. Define acceptable mobile code and mobile code technologies.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Authorize, monitor, and control the use of mobile code.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.14. Withdrawn
Technology-specific.

3.13.15. Session Authenticity
Protect the authenticity of communications sessions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.16. Withdrawn
Incorporated into 03.13.08.

3.14. System and Information Integrity

3.14.1. Flaw Remediation

a. Identify, report, and correct system flaws.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.2. Malicious Code Protection

a. Implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Update malicious code protection mechanisms as new releases are available in accordance with configuration management policies and procedures.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Configure malicious code protection mechanisms to:
   1. Perform scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed; an
   2. Block malicious code, quarantine malicious code, or take other mitigation actions in response to malicious code detection.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.3. Security Alerts, Advisories, and Directives

a. Receive system security alerts, advisories, and directives from external organizations on an ongoing basis.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Generate and disseminate internal system security alerts, advisories, and directives, as necessary.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.4. Withdrawn
Incorporated into 03.14.02.

3.14.5. Withdrawn
Addressed by 03.14.02.

3.14.6. System Monitoring

a. Monitor the system to detect:
   1. Attacks and indicators of potential attacks and
   2. Unauthorized connections.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Identify unauthorized use of the system.
Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.7. Withdrawn
Incorporated into 03.14.06.

3.14.8. Information Management and Retention
Manage and retain CUI within the system and CUI output from the system in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.15. Planning

3.15.1. Policy and Procedures

a. Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update policies and procedures [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.15.2. System Security Plan

a. Develop a system security plan that:
   1. Defines the constituent system components;
   2. Identifies the information types processed, stored, and transmitted by the system;
   3. Describes specific threats to the system that are of concern to the organization;
   4. Describes the operational environment for the system and any dependencies on or connections to other systems or system components;
   5. Provides an overview of the security requirements for the system;
   6. Describes the safeguards in place or planned for meeting the security requirements;
   7. Identifies individuals that fulfill system roles and responsibilities; and
   8. Includes other relevant information necessary for the protection of CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update the system security plan [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Protect the system security plan from unauthorized disclosure.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.15.3. Rules of Behavior

a. Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Provide rules to individuals who require access to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Review and update the rules of behavior [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.16. System and Services Acquisition

3.16.1. Security Engineering Principles

Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.16.2. Unsupported System Components

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.16.3. External System Services

a. Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.17. Supply Chain Risk Management

3.17.1. Supply Chain Risk Management Plan

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Protect the supply chain risk management plan from unauthorized disclosure.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.17.2. Acquisition Strategies, Tools, and Methods

Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.17.3. Supply Chain Requirements and Processes

a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined security requirements].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

SIGNATORY AUTHORITY

I have reviewed the System Security Plan (SSP) for <Insert Name>, and have determined that the requirements and security controls selected, and their implementation are accurate to the best of my knowledge:

Approved By:

_____ _____
External Service Provider Representative Date

Approved By:

_____ _____
_____SSA – Security Authorization Manager Date

4. RECORD OF CHANGES

Date	Description	Made By:
10-15-2024	Draft	Oyedeji Ojo -SSA

EXHIBIT C

Social Security Administration (SSA)

SYSTEM SECURITY PLAN (SSP)

FOR

SSA ESP 53 Template v1

Confidentiality: **Low**

Integrity: **Low**

Availability: **Low**

System Impact Level:

Published Date: 13 March 2024

Prepared For

Office of Information Security

REVISION HISTORY

Name	Date	Change

TABLE OF CONTENTS

1 PURPOSE 1
2 SYSTEM IDENTIFICATION 1
3 INFORMATION SYSTEM CATEGORIZATION 1
3.1 Information Types 1
3.2 Security Objectives Categorization (FIPS 199) 2
4 PROJECT PERSONNEL 2
5 LEVERAGED AUTHORIZATIONS 2
5.1 Authorization to Operate (ATO) 2
5.2 FedRAMP 2
6 SYSTEM INFORMATION 2
6.1 System Description 2
6.1.1 Architecture Description & Diagram 2
6.1.2 Network Description & Diagram 3
6.1.3 Dataflow Description & Diagram 3
6.2 System User Groups 4
7 SYSTEM ENVIRONMENT AND INVENTORY 5
7.1 System Environment 5
7.2 Equipment Inventory 5
7.2.1 Hardware 5
7.2.2 Software 5
7.3 Ports, Protocols, and Services 5
8 SYSTEM INTERCONNECTIONS 6
8.1 Internal Connections 6
8.2 External Connections 6
9 IMPLEMENTATION STATEMENTS 7
LAWS, REGULATIONS, STANDARDS AND GUIDANCE 39
ACRONYMS 41
SIGNATORY AUTHORITY 46

1 PURPOSE

This System Security Plan provides an overview of the security requirements for the SSA ESP 53 Template v1 and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed, or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity, and availability of the data transmitted, processed or stored by SSA ESP 53 Template v1.

The security safeguards implemented for SSA ESP 53 Template v1 meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures, and practices.

2 SYSTEM IDENTIFICATION

- System Name/Version Number: SSA ESP 53 Template v1/The project version was not specified for the system.
- Acronym: SSA ESP 53 Template v1
- EA Number: A project tracking number was not assigned to the system.
- System Type: Not Specified
- Agency Operated or Contractor Operated:
- PII Data (Yes/No): No
- E-Authentication Application (Yes/No): No
- Federal Tax Information (FTI) (Yes/No): No

3 INFORMATION SYSTEM CATEGORIZATION

3.1 Information Types

This section describes how the information types used by the information system are categorized for confidentiality, integrity, and availability sensitivity levels.

The following tables identify the information types that are input, stored, processed, and/or output from SSA ESP 53 Template v1. The selection of the information types is based on guidance provided by Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office Business Reference Model 2.0 and Federal Information Processing Standards (FIPS) Pub 199, Standards for Security Categorization of Federal Information and Information Systems which is based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

Information Type	Confidentiality	Integrity	Availability
Information Sharing (M-M-M)	Moderate	Moderate	Moderate

3.2 Security Objectives Categorization (FIPS 199)

Based on the information provided in section 3.1 Information Types, SSA ESP 53 Template v1 defaults to the below high-water mark.

Confidentiality: **Low**

Integrity: **Low**

Availability: **Low**

4 PROJECT PERSONNEL

The following individuals are identified as the system owner or functional proponent/advocate for this system.

Name	Role	Email	Phone Number
Not Specified	Not Specified	Not Entered	Not Entered

5 LEVERAGED AUTHORIZATIONS

5.1 Authorization to Operate (ATO)

The SSA ESP 53 Template v1 Not Specified leverage the authority of a pre-existing Federal Entity. ATOs leveraged by SSA ESP 53 Template v1 are listed in the table that follows.

Information System Name	Federal Entity	Authorization Status	Expiration Date

5.2 FedRAMP

The SSA ESP 53 Template v1 Not Specified leverage a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by SSA ESP 53 Template v1 are listed in the table that follows.

Information System Name	Service Provider Owner	Expiration Date

6 SYSTEM INFORMATION

6.1 System Description

General Description of the System Not Specified

6.1.1 Architecture Description & Diagram

6.1.2 Network Description & Diagram

6.1.3 Dataflow Description & Diagram

6.2 System User Groups

All personnel have their status categorized with a sensitivity level in accordance with PS-2.

Category	Organization	Subsystem Name	Interface	Authentication	User Groups	Authorized Privileges	Functions Performed	Internal/External
User	Not Entered	N/A	Not Specified	Not Specified	Users	Not Specified	User Functions	Not Specified
Administrator	Not Entered	N/A	Not Specified	Not Specified	Administrators	Not Specified	Administrative Functions	Not Specified

There are currently internal personnel and external personnel. Within one year, it is anticipated that there will be internal personnel and external personnel.

7 SYSTEM ENVIRONMENT AND INVENTORY

When completed, SSA will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial Plan of Actions & Milestones (POA&M)
- Quarterly Continuous Monitoring (POA&M or as a separate document)

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 5 CM-8.

7.1 System Environment

Location	City	State
ACI-AWS	Not Entered	Not Entered
E-Vault (E-V)	Not Entered	Colorado
Kansas City Service Delivery Point (KS SDP)	Kansas City	Missouri
National Support Center (NSC)	Urbana	Maryland
Richmond Service Delivery Point (RI SDP)	Richmond	California
Secondary Support Center (SSC)	Durham	North Carolina

7.2 Equipment Inventory

7.2.1 Hardware

Hostname	Manufacturer/Model	Operating System/Version	Function

Note: IPv4 and IPv6 are only entered if applicable.

7.2.2 Software

Name	Version	Vendor	Use/Description

7.3 Ports, Protocols, and Services

Entity	Description/Service	Direction	Service	TCP/UDP	Port Number
Not Specified	Not Specified	Not Specified	Not Specified	Not Specified	

8 SYSTEM INTERCONNECTIONS

8.1 Internal Connections

System Acronym	System Name	Data Sharing Method	Data Type	Data Description	Security Categorization
Not Specified	Not Specified	Not Specified	Not Specified	Not Specified	Not Specified

8.2 External Connections

System Acronym	System Name	Data Sharing Method	Data Type	Data Description	Security Categorization
Not Specified	Not Specified	Not Specified	Not Specified	Not Specified	Not Specified

9 IMPLEMENTATION STATEMENTS

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
AC-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.d.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.d.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.d.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.h.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
AC-2.h.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.h.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.i.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.i.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.i.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.j	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.k	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.l	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-7.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-7.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.a.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
AC-8.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.c.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-14.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-14.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-17.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-17.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-18.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-18.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-19.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-19.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-20.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-20.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-20.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-22.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-22.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-22.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-22.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
AT-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-2(2)	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low impact.
AT-2.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-2.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-3.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-3.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
AT-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-2.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-3.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-3.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-3.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
AU-3.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-6.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-8.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-8.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-9.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-9.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-11	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-12.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-12.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-12.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
CA-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.b.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.b.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.b.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-3.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
CA-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-6.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-6.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-6.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-6.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7(4).a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7(4).b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7(4).c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-9.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
CA-9.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-9.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-9.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-2.b.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-2.b.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-2.b.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-5	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low impact.
CM-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
CM-6.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-6.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-7.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-7.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-8.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-8.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-8.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-8.a.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-8.a.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-8.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-10.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-10.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-10.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-11.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-11.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-11.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
CP-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
CP-2.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.h	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-3.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-3.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-3.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-9.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-9.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-9.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-9.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
IA-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-2(1)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-2(2)	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low impact.
IA-2(8)	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low impact.
IA-2(12)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
IA-5(1).f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).h	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.h	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.i	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-8(1)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-8(2).a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
IA-8(2).b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-8(4)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-11	System-Specific	Not Entered	Not Assigned	-	-	-	-	IA (Identification and Authentication) controls and additional control enhancements are not required.
IR-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-2.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-2.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-2.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
IR-5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
IR-8.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-2.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-2.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
MA-4.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-5.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-7.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-7.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
PE-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
PE-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-6.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-8.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-8.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-8.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-12	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-13	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-14.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-14.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-15	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-16.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-16.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
PL-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.11	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.12	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.13	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.14	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.15	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
PL-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4(1).a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4(1).b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4(1).c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-11	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
PS-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-3.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-4.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-5.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-5.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
PS-6.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-6.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-7.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-7.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-7.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-7.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-7.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-8.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-8.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
RA-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3(1).a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3(1).b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5(2)	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low impact.
RA-5(11)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.b.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.b.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
RA-5.b.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-3.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
SA-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-3.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4(10)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.h	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.i	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.b.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.b.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
SA-5.b.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-8	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low impact.
SA-9.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-9.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-9.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-22.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SA-22.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SC-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
SC-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-7.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-7.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-7.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-12	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-13.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-13.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-15.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-15.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-20.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-20.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-21	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-22	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-39	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
SI-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-3.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-3.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-3.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-3.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
SI-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-5.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-5.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-12	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low or moderate-impact.
SR-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-2(1)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
SR-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-3.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-5	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-8	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-10	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-11(1)	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-11(2)	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-11.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-11.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-12	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.

LAWS, REGULATIONS, STANDARDS AND GUIDANCE

- Computer Fraud and Abuse Act, 18 U.S.C. 1030
- E-Government Act (Public Law 107-347), Title III, Federal Information Security Modernization Act (FISMA)
- Federal Information System Controls Audit Manual (FISCAM)
- Federal Information Security Modernization Act of 2014 (FISMA 2014)
- Freedom of Information Act 5 U.S.C 552
- Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection
- Information Security Policy (ISP) for the Social Security Administration (SSA) Handbook
- NIST FIPS 140-2, Security Requirements for Cryptographic Modules
- NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors
- NIST SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-27 Rev. A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST SP 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-60 Vol. 1 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories

- NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide
- NIST SP 800-63-3, Digital Identity Guidelines
- NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle
- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-145, The NIST Definition of Cloud Computing
- OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act
- OMB Circular A-123, Management's Responsibility for Internal Control
- OMB Circular A-130, Managing Information as a Strategic Resource
- OMB Federal Enterprise Architecture Framework Version 2
- OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
- OMB M-04-04, E-Authentication Guidance for Federal Agencies
- OMB M-06-16, Protection of Sensitive Agency Information
- OMB M-17-15, Rescission of Memoranda Relating to Identity Management
- Privacy Act of 1974, 5 U.S.C 552.a
- Records Management by Federal Agencies, 44 U.S.C. 31
- Trade Secrets Act, 18 U.S.C. 1905, Disclosure of confidential information generally

ACRONYMS

Acronym	Definition
3PAO	Third-Party Assessment Organization
AC	Associate Commissioner
AC	Access Control
ACL	Access Control List
ACTR	Access Control Test Report
ALM	Application Lifecycle Management
AMB	Access Management Branch
AO	Authorizing Official
APM	Application Portfolio Management
APP	Application
ARB	Architecture Review Board
AT	Awareness Training
ATO	Authorization to Operate
AU	Audit and Accountability
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BII	Business Identifiable Information
BITS	Batch Integration Test System
BPD	Business Process Description
BPM	Business Project Manager
BRM	Business Reference Model
BSM	Boundary Scope Memorandum
CA	Security Assessment and Authorization
CAPRS	Change Asset Problem Reporting System
CCB	Configuration Control Board
CCCP	Configuration Change Control Process
CET	Customer Engagement Tool
CI	Configuration Items
CICS	Customer Information Control System
CIO	Chief Information Officer
CIRT	Cyber Incident Response Team
CISO	Chief Information Security Officer
CM	Configuration Management
CMP	Configuration Management Plan
COOP	Continuity of Operations Plan
COPPA	Children's Online Privacy Protection Act
COR	Contracting Officer Representative
COTS	Commercial Off The Shelf
CP	Contingency Planning
CPPs	Contingency Planning Policies
CR	Change Request
CSAM	Cybersecurity Assessment and Management

Acronym	Definition
CSO	Chief Security Officer
CUI	Confidential Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DASD	Direct Access Storage Devices
DB	Database
DBMS	Database Management System
DBOPC	Division of Batch Operation Production Control
DCA	Division of Compliance and Authorization
DCS	Deputy Commissioner for Systems
DDBS	Division of Database Systems
DESEI	Division of Enterprise Software Engineering Infrastructure
DFR	Detailed Functional Requirements
DIET	Division of Integration and Environmental Testing
DIIAS	Division of Internet/Intranet Application Services
DISSAO	Division of Information Systems Security Administration and Operations
DMSS	Division of Mainframe System Software
DMZ	Demilitarized Zone
DNE	Division of Network Engineering
DOSDO	Division of Online Systems and Database Operations
DR	Disaster Recovery
DRE	Disaster Recovery Exercise
DRMA	Division of Resource Management and Acquisition
DRP	Disaster Recovery Plan
DSE	Division of Security Engineering
DSPSM	Division of Systems Performance and Service-level Management
DSS	Detailed System Specifications
DSSM	Division of Systems Storage Management
DSUSF	Division of Systems User Services and Facilities
DTO	Division of Technical Operations
EIC	Enterprise Inheritable Controls
EMATS	Emergency Memo and Tracking System
EPO	McAfee ePolicy Orchestrator
EWANS	Enterprise Wide Mainframe & Distributed Network Telecommunications Services and System
FIPS	Federal Information Processing Standards
FISCAM	Federal Information Controls Systems Audit Manual
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FTI	Federal Tax Information
FTP	File Transfer Protocol
FTP	Functional Test Plan
GSS	General Support System
HIDS	Host-based Intrusion Detection System

Acronym	Definition
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
HW	Hardware
IA	Independent Assessor
IA	Identification and Authentication
IATO	Interim Authorization to Operate
ID	Identification
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
IR	Incident Response
IRP	Incident Response Plan
IRS	Internal Revenue Service
ISA	Interconnection Security Agreement
ISCP	Information Security Contingency Plan
ISP	Information Security Policy
ISP	Internet Service Provider
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
IV&V	Independent Verification & Validation
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LIS	Low Income Subsidy
LLC	Limited Liability Company
MA	Major Application
MA	Maintenance
MDAB	Mainframe Data Assurance Branch
MKS	Mortice Kern Systems
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection
MTD	Maximum Tolerable Downtime
MTP	Master Training Plan
MySSA	My Social Security
NDA	Non-Disclosure Agreement
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standards and Technology
NMS	Network Management System
NSC	National Support Center
OASSIS	Office of Applications and Supplemental Security Income Systems
OBFM	Office of Budget, Finance, and Management
OBIS	Office of Benefit Information Systems
OEEAS	Office of Earnings, Enumeration, and Administrative Systems

Acronym	Definition
OEP	Occupant Emergency Plan
OESAE	Office of Enterprise Support, Architecture & Engineering
OFM	Office of Facilities Management
OIS	Office of Information Security
OMB	Office of Management and Budget
OOS	Office of Systems
OPD	Office of Privacy and Disclosure
ORSIS	Office of Retirement and Survivors Insurance Systems
OS	Operating System
OSES	Office of Systems Electronic Services
OSOHE	Office of System Operations and Hardware Engineering
OSRF	Online Software Release Form
OSSF	Offsite Secure Storage Facility
OSSMB	Open Systems Storage Management Branch
OTSO	Office of Telecommunications and System Operations
P&A	Planning and Analysis
PCCB	Project Configuration Control Board
PCM	Project Configuration Manager
PDA	Personal Digital Assistant
PE	Physical and Environmental Protection
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PL	Public Law
PL	Planning
PM	Program Manager
PMC	Product Monitoring and Control
POA&M	Plan of Actions and Milestones
POC	Point of Contact
PR	Problem Report
PRIDE	Project Resource Guide
PS	Personnel Security
PSA	Project Scope Agreement
PSC	Program Service Centers
PSMA	Project Scope Management Agreement
PTA	Privacy Threshold Analysis
QA2	Quality Assurance System
RA	Risk Assessment or Risk Assessor
RA	Risk Assessment
RAR	Risk Assessment Report
RMF	Risk Management Framework
ROE	Rules of Engagement
RPO	Recovery Point Objective
rPSA	Release-Specific Project Scope Agreement
RSDI	Retirement, Survivor, or Disability Insurance

Acronym	Definition
RTO	Recovery Time Objective
SA	System and Services Acquisition
SA&A	Security Assessment and Authorization
SAM	Security Authorization Manager
SAP	System Assessment Plan, Security Authorization Package
SAR	Security Assessment Report
SAS	Security Assessment Services
SBU	Sensitive But Unclassified
SC	System and Communications Protection
SCA	Security Control Assessment
SCDF	Significant Change Determination Form
SCQ	Significant Change Questionnaire
SDLC	Systems Development Lifecycle
SDP	Systems Development Plan
SEPG	Software Engineering Process Group
SI	System and Information Integrity
SIA	Security Impact Analysis
SITAR	Strategic Information Technology Assessment Review
SME	Subject Matter Expert
SO	System Owner
SOC	Security Operations Center
SORN	System of Records Notice
SP	Special Publication
SPM	System Project Manager
SR	Service Request
SRC	Systems Release Certification
SSA	Social Security Administration
SSC	Second Support Center
SSP	System Security Plan
SW	Software
UATPA	User Acceptance Test Plan Agreement
URL	Uniform Resource Locator
V-HW	Virtual Hardware
VPN	Virtual Private Network

SIGNATORY AUTHORITY

The SSP will be reviewed at least annually or whenever a significant change occurs. Modifications to the SSP must occur within Xacta 360 and be signed by all applicable parties.

Role
SAM - Security Authorization Manager

EXHIBIT D

Social Security Administration (SSA)

SYSTEM SECURITY PLAN (SSP)

FOR

SSA ESP 171 Template v1

Confidentiality: **Low**

Integrity: **Low**

Availability: **Low**

System Impact Level:

Published Date: 13 March 2024

Prepared For

Office of Information Security

REVISION HISTORY

Name	Date	Change

TABLE OF CONTENTS

1 PURPOSE 1
2 SYSTEM IDENTIFICATION 1
3 INFORMATION SYSTEM CATEGORIZATION 1
3.1 Information Types 1
3.2 Security Objectives Categorization (FIPS 199) 2
4 PROJECT PERSONNEL 2
5 LEVERAGED AUTHORIZATIONS 2
5.1 Authorization to Operate (ATO) 2
5.2 FedRAMP 2
6 SYSTEM INFORMATION 2
6.1 System Description 2
6.1.1 Architecture Description & Diagram 2
6.1.2 Network Description & Diagram 3
6.1.3 Dataflow Description & Diagram 3
6.2 System User Groups 4
7 SYSTEM ENVIRONMENT AND INVENTORY 5
7.1 System Environment 5
7.2 Equipment Inventory 5
7.2.1 Hardware 5
7.2.2 Software 5
7.3 Ports, Protocols, and Services 5
8 SYSTEM INTERCONNECTIONS 6
8.1 Internal Connections 6
8.2 External Connections 6
9 IMPLEMENTATION STATEMENTS 7
LAWS, REGULATIONS, STANDARDS AND GUIDANCE 14
ACRONYMS 16
SIGNATORY AUTHORITY 21

1 PURPOSE

This System Security Plan provides an overview of the security requirements for the SSA ESP 171 Template v1 and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed, or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity, and availability of the data transmitted, processed or stored by SSA ESP 171 Template v1.

The security safeguards implemented for SSA ESP 171 Template v1 meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures, and practices.

2 SYSTEM IDENTIFICATION

- System Name/Version Number: SSA ESP 171 Template v1/The project version was not specified for the system.
- Acronym: SSA ESP 171 Template v1
- EA Number: A project tracking number was not assigned to the system.
- System Type: Not Specified
- Agency Operated or Contractor Operated:
- PII Data (Yes/No): No
- E-Authentication Application (Yes/No): No
- Federal Tax Information (FTI) (Yes/No): No

3 INFORMATION SYSTEM CATEGORIZATION

3.1 Information Types

This section describes how the information types used by the information system are categorized for confidentiality, integrity, and availability sensitivity levels.

The following tables identify the information types that are input, stored, processed, and/or output from SSA ESP 171 Template v1. The selection of the information types is based on guidance provided by Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office Business Reference Model 2.0 and Federal Information Processing Standards (FIPS) Pub 199, Standards for Security Categorization of Federal Information and Information Systems which is based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

Information Type	Confidentiality	Integrity	Availability
Statistical Information	Moderate	Moderate	Moderate

3.2 Security Objectives Categorization (FIPS 199)

Based on the information provided in section 3.1 Information Types, SSA ESP 171 Template v1 defaults to the below high-water mark.

Confidentiality: **Low**

Integrity: **Low**

Availability: **Low**

4 PROJECT PERSONNEL

The following individuals are identified as the system owner or functional proponent/advocate for this system.

Name	Role	Email	Phone Number
Not Specified	Not Specified	Not Entered	Not Entered

5 LEVERAGED AUTHORIZATIONS

5.1 Authorization to Operate (ATO)

The SSA ESP 171 Template v1 Not Specified leverage the authority of a pre-existing Federal Entity. ATOs leveraged by SSA ESP 171 Template v1 are listed in the table that follows.

Information System Name	Federal Entity	Authorization Status	Expiration Date

5.2 FedRAMP

The SSA ESP 171 Template v1 Not Specified leverage a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by SSA ESP 171 Template v1 are listed in the table that follows.

Information System Name	Service Provider Owner	Expiration Date

6 SYSTEM INFORMATION

6.1 System Description

General Description of the System Not Specified

6.1.1 Architecture Description & Diagram

6.1.2 Network Description & Diagram

6.1.3 Dataflow Description & Diagram

6.2 System User Groups

All personnel have their status categorized with a sensitivity level in accordance with PS-2.

Category	Organization	Subsystem Name	Interface	Authentication	User Groups	Authorized Privileges	Functions Performed	Internal/External
Administrator	Not Entered	N/A	Not Specified	Not Specified	Administrators	Not Specified	Administrative Functions	Not Specified
User	Not Entered	N/A	Not Specified	Not Specified	Users	Not Specified	User Functions	Not Specified

There are currently internal personnel and external personnel. Within one year, it is anticipated that there will be internal personnel and external personnel.

7 SYSTEM ENVIRONMENT AND INVENTORY

When completed, SSA will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial Plan of Actions & Milestones (POA&M)
- Quarterly Continuous Monitoring (POA&M or as a separate document)

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

7.1 System Environment

Location	City	State
ACI-AWS	Not Entered	Not Entered
E-Vault (E-V)	Not Entered	Colorado
Kansas City Service Delivery Point (KS SDP)	Kansas City	Missouri
National Support Center (NSC)	Urbana	Maryland
Richmond Service Delivery Point (RI SDP)	Richmond	California
Secondary Support Center (SSC)	Durham	North Carolina

7.2 Equipment Inventory

7.2.1 Hardware

Hostname	Manufacturer/Model	Operating System/Version	Function

Note: IPv4 and IPv6 are only entered if applicable.

7.2.2 Software

Name	Version	Vendor	Use/Description

7.3 Ports, Protocols, and Services

Entity	Description/Service	Direction	Service	TCP/UDP	Port Number
Not Specified	Not Specified	Not Specified	Not Specified	Not Specified	

8 SYSTEM INTERCONNECTIONS

8.1 Internal Connections

System Acronym	System Name	Data Sharing Method	Data Type	Data Description	Security Categorization
Not Specified	Not Specified	Not Specified	Not Specified	Not Specified	Not Specified

8.2 External Connections

System Acronym	System Name	Data Sharing Method	Data Type	Data Description	Security Categorization
Not Specified	Not Specified	Not Specified	Not Specified	Not Specified	Not Specified

9 IMPLEMENTATION STATEMENTS

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.1.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.11	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.12	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.13	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.14	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.15	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.16	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.1.17	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.18	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.19	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.20	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.21	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.22	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.2.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.2.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.2.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.3.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.5.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.11	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.6.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.6.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.6.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.7.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.7.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.7.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.7.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.7.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.7.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.8.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.9.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.9.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.10.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.10.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.10.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.10.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.10.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.10.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.11.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.11.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.11.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.12.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.12.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.12.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.11	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.12	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.13	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.14	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.15	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.13.16	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

LAWS, REGULATIONS, STANDARDS AND GUIDANCE

- Computer Fraud and Abuse Act, 18 U.S.C. 1030
- E-Government Act (Public Law 107-347), Title III, Federal Information Security Modernization Act (FISMA)
- Federal Information System Controls Audit Manual (FISCAM)
- Federal Information Security Modernization Act of 2014 (FISMA 2014)
- Freedom of Information Act 5 U.S.C 552
- Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection
- Information Security Policy (ISP) for the Social Security Administration (SSA) Handbook
- NIST FIPS 140-2, Security Requirements for Cryptographic Modules
- NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors
- NIST SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-27 Rev. A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-60 Vol. 1 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories

- NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide
- NIST SP 800-63-3, Digital Identity Guidelines
- NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle
- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-145, The NIST Definition of Cloud Computing
- OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act
- OMB Circular A-123, Management's Responsibility for Internal Control
- OMB Circular A-130, Managing Information as a Strategic Resource
- OMB Federal Enterprise Architecture Framework Version 2
- OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
- OMB M-04-04, E-Authentication Guidance for Federal Agencies
- OMB M-06-16, Protection of Sensitive Agency Information
- OMB M-17-15, Rescission of Memoranda Relating to Identity Management
- Privacy Act of 1974, 5 U.S.C 552.a
- Records Management by Federal Agencies, 44 U.S.C. 31
- Trade Secrets Act, 18 U.S.C. 1905, Disclosure of confidential information generally

ACRONYMS

Acronym	Definition
3PAO	Third-Party Assessment Organization
AC	Associate Commissioner
AC	Access Control
ACL	Access Control List
ACTR	Access Control Test Report
ALM	Application Lifecycle Management
AMB	Access Management Branch
AO	Authorizing Official
APM	Application Portfolio Management
APP	Application
ARB	Architecture Review Board
AT	Awareness Training
ATO	Authorization to Operate
AU	Audit and Accountability
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BII	Business Identifiable Information
BITS	Batch Integration Test System
BPD	Business Process Description
BPM	Business Project Manager
BRM	Business Reference Model
BSM	Boundary Scope Memorandum
CA	Security Assessment and Authorization
CAPRS	Change Asset Problem Reporting System
CCB	Configuration Control Board
CCCP	Configuration Change Control Process
CET	Customer Engagement Tool
CI	Configuration Items
CICS	Customer Information Control System
CIO	Chief Information Officer
CIRT	Cyber Incident Response Team
CISO	Chief Information Security Officer
CM	Configuration Management
CMP	Configuration Management Plan
COOP	Continuity of Operations Plan
COPPA	Children's Online Privacy Protection Act
COR	Contracting Officer Representative
COTS	Commercial Off The Shelf
CP	Contingency Planning
CPPs	Contingency Planning Policies
CR	Change Request
CSAM	Cybersecurity Assessment and Management

Acronym	Definition
CSO	Chief Security Officer
CUI	Confidential Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DASD	Direct Access Storage Devices
DB	Database
DBMS	Database Management System
DBOPC	Division of Batch Operation Production Control
DCA	Division of Compliance and Authorization
DCS	Deputy Commissioner for Systems
DDBS	Division of Database Systems
DESEI	Division of Enterprise Software Engineering Infrastructure
DFR	Detailed Functional Requirements
DIET	Division of Integration and Environmental Testing
DIIAS	Division of Internet/Intranet Application Services
DISSAO	Division of Information Systems Security Administration and Operations
DMSS	Division of Mainframe System Software
DMZ	Demilitarized Zone
DNE	Division of Network Engineering
DOSDO	Division of Online Systems and Database Operations
DR	Disaster Recovery
DRE	Disaster Recovery Exercise
DRMA	Division of Resource Management and Acquisition
DRP	Disaster Recovery Plan
DSE	Division of Security Engineering
DSPSM	Division of Systems Performance and Service-level Management
DSS	Detailed System Specifications
DSSM	Division of Systems Storage Management
DSUSF	Division of Systems User Services and Facilities
DTO	Division of Technical Operations
EIC	Enterprise Inheritable Controls
EMATS	Emergency Memo and Tracking System
EPO	McAfee ePolicy Orchestrator
EWANS	Enterprise Wide Mainframe & Distributed Network Telecommunications Services and System
FIPS	Federal Information Processing Standards
FISCAM	Federal Information Controls Systems Audit Manual
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FTI	Federal Tax Information
FTP	File Transfer Protocol
FTP	Functional Test Plan
GSS	General Support System
HIDS	Host-based Intrusion Detection System

Acronym	Definition
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
HW	Hardware
IA	Independent Assessor
IA	Identification and Authentication
IATO	Interim Authorization to Operate
ID	Identification
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
IR	Incident Response
IRP	Incident Response Plan
IRS	Internal Revenue Service
ISA	Interconnection Security Agreement
ISCP	Information Security Contingency Plan
ISP	Information Security Policy
ISP	Internet Service Provider
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
IV&V	Independent Verification & Validation
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LIS	Low Income Subsidy
LLC	Limited Liability Company
MA	Major Application
MA	Maintenance
MDAB	Mainframe Data Assurance Branch
MKS	Mortice Kern Systems
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection
MTD	Maximum Tolerable Downtime
MTP	Master Training Plan
MySSA	My Social Security
NDA	Non-Disclosure Agreement
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standards and Technology
NMS	Network Management System
NSC	National Support Center
OASSIS	Office of Applications and Supplemental Security Income Systems
OBFM	Office of Budget, Finance, and Management
OBIS	Office of Benefit Information Systems
OEEAS	Office of Earnings, Enumeration, and Administrative Systems

Acronym	Definition
OEP	Occupant Emergency Plan
OESAE	Office of Enterprise Support, Architecture & Engineering
OFM	Office of Facilities Management
OIS	Office of Information Security
OMB	Office of Management and Budget
OOS	Office of Systems
OPD	Office of Privacy and Disclosure
ORSIS	Office of Retirement and Survivors Insurance Systems
OS	Operating System
OSES	Office of Systems Electronic Services
OSOHE	Office of System Operations and Hardware Engineering
OSRF	Online Software Release Form
OSSF	Offsite Secure Storage Facility
OSSMB	Open Systems Storage Management Branch
OTSO	Office of Telecommunications and System Operations
P&A	Planning and Analysis
PCCB	Project Configuration Control Board
PCM	Project Configuration Manager
PDA	Personal Digital Assistant
PE	Physical and Environmental Protection
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PL	Public Law
PL	Planning
PM	Program Manager
PMC	Product Monitoring and Control
POA&M	Plan of Actions and Milestones
POC	Point of Contact
PR	Problem Report
PRIDE	Project Resource Guide
PS	Personnel Security
PSA	Project Scope Agreement
PSC	Program Service Centers
PSMA	Project Scope Management Agreement
PTA	Privacy Threshold Analysis
QA2	Quality Assurance System
RA	Risk Assessment or Risk Assessor
RA	Risk Assessment
RAR	Risk Assessment Report
RMF	Risk Management Framework
ROE	Rules of Engagement
RPO	Recovery Point Objective
rPSA	Release-Specific Project Scope Agreement
RSDI	Retirement, Survivor, or Disability Insurance

Acronym	Definition
RTO	Recovery Time Objective
SA	System and Services Acquisition
SA&A	Security Assessment and Authorization
SAM	Security Authorization Manager
SAP	System Assessment Plan, Security Authorization Package
SAR	Security Assessment Report
SAS	Security Assessment Services
SBU	Sensitive But Unclassified
SC	System and Communications Protection
SCA	Security Control Assessment
SCDF	Significant Change Determination Form
SCQ	Significant Change Questionnaire
SDLC	Systems Development Lifecycle
SDP	Systems Development Plan
SEPG	Software Engineering Process Group
SI	System and Information Integrity
SIA	Security Impact Analysis
SITAR	Strategic Information Technology Assessment Review
SME	Subject Matter Expert
SO	System Owner
SOC	Security Operations Center
SORN	System of Records Notice
SP	Special Publication
SPM	System Project Manager
SR	Service Request
SRC	Systems Release Certification
SSA	Social Security Administration
SSC	Second Support Center
SSP	System Security Plan
SW	Software
UATPA	User Acceptance Test Plan Agreement
URL	Uniform Resource Locator
V-HW	Virtual Hardware
VPN	Virtual Private Network

SIGNATORY AUTHORITY

The SSP will be reviewed at least annually or whenever a significant change occurs. Modifications to the SSP must occur within Xacta 360 and be signed by all applicable parties.

Role
SAM - Security Authorization Manager

EXHIBIT E

Attachment A. (GAM 15.02) Worksheet for Reporting Loss or Potential Loss of PII

The "Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information" is intended to assist you to quickly organize and report the needed information about the potential incident.

1. Information about the individual making the report to the NNSC:

Name:					
Position:					
Deputy Commissioner Level Organization:					
Phone Numbers:					
Work:		Cell:		Home/Other:	
Email Address:					
Check one of the following:					
Management Official		Security Officer		Non-Management	

2. Information about the data that was lost/stolen:

Describe what was lost or stolen (e.g., case file, MBR data):

Which element(s) of PII did the data contain?

Name		Bank Account Info	
SSN		Medical/Health Information	
Date of Birth		Benefit Payment Info	
Place of Birth		Mother's Maiden Name	
Address		Other (describe):	

Estimated volume of records involved:

3. How was the data physically stored, packaged and/or contained?

Paper or Electronic? (Circle one):

If Electronic, what type of device?

Laptop		USB Drive		Backup Tape		Blackberry	
Workstation		Server		CD/DVD		Mobile Phone #	
Hard Drive		Floppy Disk		Cell (not Blackberry)			
Other (describe):							

Additional Questions if Electronic:

								Yes	No	Not Sure
a. Was the device encrypted?										
b. Was the device password protected?										
c. If a laptop, was a VPN SmartCard lost?										
d. If laptop, powerstate when	Off		Sleep		Hibernate		Not			

lost?							Sure	
Cardholder's Name:								
Cardholder's SSA logon PIN:								
Hardware Make/Model:								
Hardware Serial Number:								

Additional Questions if Paper:

	Yes	No	Not Sure
a. Was the information in a locked briefcase?			
b. Was the information in a locked cabinet or drawer?			
c. Was the information in a locked vehicle trunk?			
d. Was the information redacted?			
e. Other circumstances:			

4. If the employee/contractor who was in possession of the data or to whom the data was assigned is not the person making the report to the NNSC (as listed in #1), information about this employee/contractor:

Name:					
Position:					
Deputy Commissioner Level Organization:					
Phone Numbers:					
Work:		Cell:		Home/Other:	
Email Address:					

5. Circumstances of the loss:

a. When was it lost/stolen:

b. Brief description of how the loss/theft occurred:

c. When was it reported to SSA management official (date and time)?

6. Have any other SSA components been contacted? If so, who? (Include deputy commissioner level, agency level, regional/associate level component names)

7. Which reports have been filed? (include FPS, local police, and SSA reports)

Report Filed	Yes	No	Report Number
Federal Protective Service			
Local Police			
OIG			

	Yes	No
SSA-3114 (Incident Alert)		
SSA-342 (Report of Survey)		
Security Assessments and Funded Enhancements (SAFE)		

Other (describe)

8. **Other pertinent information (include actions underway as well as any contacts with other agencies, law enforcement or the press):**

EXHIBIT F

GENERAL RECORDS SCHEDULE 4.2: Information Access and Protection Records

This schedule covers records created in the course of agencies (1) responding to requests for access to Government information and (2) protecting information that is classified or controlled unclassified, or contains personal data that is required by law to be protected.

Agencies must offer any records created prior to January 1, 1921, to the National Archives and Records Administration (NARA) before applying disposition instructions in this schedule.

Item	Records Description	Disposition Instruction	Disposition Authority
001	**FOIA, Privacy Act, and classified documents administrative records.** Records on managing information access and protection activities. Records include: • correspondence related to routine implementation of the FOIA and Privacy Act and administration of document security classification • associated subject files • feeder and statistical reports **Exclusion:** This item does not cover records documenting policies and procedures accumulated in offices having agency-wide responsibilities for FOIA, Privacy Act, and classified documents. These records must be scheduled by the agency on an agency-specific schedule.	**Temporary.** Destroy when 3 years old, but longer retention is authorized if needed for business use.	DAA-GRS-2019-0001-0001
010	**General information request files.** Requests for information, publications, photographs, and other information involving no administrative action, policy decision, or special compilations or research. Also includes acknowledgements, replies, and referrals of inquiries to other offices for response.	**Temporary**. Destroy when 90 days old, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0001
020	**Access and disclosure request files**. Case files created in response to requests for information under the Freedom of Information Act (FOIA), Mandatory Declassification Review (MDR) process, Privacy Act (PA), Classification Challenge, and similar access programs, and completed by: • granting the request in full • granting the request in part • denying the request for any reason including: o inability to fulfill request because records do not exist o inability to fulfill request because request inadequately describes records	**Temporary**. Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later, but longer retention is authorized if required for business use.	DAA-GRS-2016-0002-0001

Item	Records Description		Disposition Instruction	Disposition Authority
	○ inability to fulfill request because search or reproduction fees are not paid • final adjudication on appeal to any of the above original settlements • final agency action in response to court remand on appeal Includes: • requests (either first-party or third-party) • replies • copies of requested records • administrative appeals • related supporting documents (such as sanitizing instructions) **Note 1**: Record copies of requested records remain covered by their original disposal authority, but if disposable sooner than their associated access/disclosure case file, may be retained under this item for disposition with that case file. **Note 2**: Agencies may wish to retain redacted copies of requested records for business use after the rest of the associated request case file is destroyed.			
030	**Information access and protection operational records**.	**Records tracking and controlling access to protected information.** Includes: • records documenting receipt, internal routing, dispatch, or destruction of classified and controlled unclassified records • tracking databases and other records used to manage overall access program • requests and authorizations for individuals to have access to classified and controlled unclassified records and information **Note**: Records documenting individuals' security clearances are covered under GRS 5.6, items 180 and 181.	**Temporary**. Destroy 2 years after last form entry, reply, or submission; or when associated documents are declassified, decontrolled, or destroyed; or when an individual's authorization expires; whichever is appropriate. Longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0002
031		**Access control records.** Includes: • safe and padlock combinations • names or other personal identifiers of individuals who know combinations	**Temporary**. Destroy when superseded or obsolete, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0020

Item	Records Description		Disposition Instruction	Disposition Authority
		• comparable data used to control access into classified document containers		
032		**Records relating to classified or controlled unclassified document containers.** Includes forms placed on safes, cabinets, or vaults that record opening, closing, and routine checking of container security, such as SF-701 and SF-702. **Note**: Forms involved in investigations are not covered by this item. They are instead retained according to the schedule item for records of the investigation.	**Temporary**. Destroy 90 days after last entry on form, but longer retention is authorized if required for business use.	DAA-GRS-2016-0002-0003
040	**Records of accounting for and controlling access to records requested under FOIA, PA, and MDR**. Records documenting identity of, and internal routing, control points, and accountability for information to which access has been requested. Includes: • forms, registers, ledgers, logs, and tracking systems documenting requester identity and contact information, request date, and nature or purpose of request • inventories • forms accompanying documents to ensure continuing control, showing names of people handling the documents, inter-office routing, and comparable data • agent and researcher files		**Temporary**. Destroy 5 years after date of last entry or final action by agency, as appropriate, but longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0003
050	**Privacy Act accounting of disclosure files**. Files maintained under the provisions of 5 U.S.C. §552a(c) for an accurate accounting of the date, nature, and purpose of each disclosure of a record to any person or to another agency. Includes: • forms with the subject individual's name • records of the requester's name and address • explanations of the purpose for the request • date of disclosure • proof of subject individual's consent		**Temporary**. Dispose of in accordance with the approved disposition instructions for the related subject individual's records, or 5 years after the disclosure for which the accountability was made, whichever is later.	NC1-64-77-1 item 27

Item	Records Description		Disposition Instruction	Disposition Authority
060	**Erroneous release records**. Files relating to the inadvertent release of privileged information to unauthorized parties, containing information the disclosure of which would constitute an unwarranted invasion of personal privacy. Includes: • requests for information • copies of replies • all related supporting documents May include: • official copy of records requested or copies	**Records filed with the record-keeping copy of the erroneously released records.**	**Temporary**. Follow the disposition instructions approved for the released record copy or destroy 6 years after the erroneous release, whichever is later.	DAA-GRS-2015-0002-0001
061		**Records filed separately from the record-keeping copy of the released records.**	**Temporary**. Destroy 6 years after the erroneous release, but longer retention is authorized if required for business use.	DAA-GRS-2015-0002-0002
065	**Privacy complaint files**. Records of privacy complaints (and responses) agencies receive in these categories: • process and procedural (consent, collection, and appropriate notice) • redress (inquiries seeking resolution of difficulties or concerns about privacy matters not specifically outlined in the Privacy Act) • operational (inquiries regarding Privacy Act matters but not including Privacy Act requests for access and/or correction) • complaints referred to another organization		**Temporary**. Destroy 3 years after resolution or referral, as appropriate, but longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0004
070	**Agency reports to the Congress, Department of Justice, or other entities regarding FOIA, MDR, PA, and similar access and disclosure programs.** **Note**: This item does not apply to summary reports incorporating government-wide statistics. These must be scheduled separately by the summarizing agent.		**Temporary**. Destroy 2 years after date of report, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0006
080	**Legal and regulatory compliance reporting records.** Reports prepared in compliance with Federal laws and regulations, such as the E-Government Act (Public Law 107-347), Federal Information Security Modernization Act of 2014, and Title V (Confidential Information	**Annual reports by agency CIO, Inspector General, or Senior Agency Official for Privacy.** **Legal citation**: OMB M-07-16.	**Temporary**. Destroy 5 years after submission of report, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0022

Item	Records Description		Disposition Instruction	Disposition Authority
081	Protection and Statistical Efficiency Act), as codified in 44 U.S.C. §101.	**All other agency reports and internal reports by individual system owners to the Senior Agency Official for Privacy (SAOP).**	**Temporary**. Destroy 2 years after submission of report, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0023
090	**Privacy Act amendment request files.** Files relating to an individual's request to amend a record pertaining to that individual under 5 U.S.C. §552a(d)(2), to the individual's request for review of an agency's refusal to amend a record under 5 U.S.C. §552a(d)(3), and to any civil action or appeal brought by the individual against the refusing agency under 5 U.S.C. §552a(g). Includes: • requests to amend and to review refusal to amend • copies of agency's replies • statement of disagreement • agency justification for refusal to amend a record • appeals • related materials		**Temporary**. Destroy with the records for which amendment was requested or 4 years after close of case (final determination by agency or final adjudication, whichever applies), whichever is later. Longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0007
100	**Automatic and systematic declassification review program records**. Files related to the review of permanent records in anticipation of automatic declassification at 25, 50, or 75 years per Executive Order 13526, and the periodic review of records exempted from automatic declassification. Files include program records documenting declassification decisions.		**Temporary**. Destroy or delete 30 years after completion of review, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0008
110	**Fundamental classification guidance review files.** Reports, significant correspondence, drafts, received comments, and related materials responding to "fundamental classification guidance review" as required by Executive Order 13526 Section 1.9. **Note**: This item does not cover reports and correspondence received at the Information Security Oversight Office (ISOO).		**Temporary**. Destroy 5 years after report is submitted to ISOO, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0011
120	**Classified information nondisclosure agreements**. Copies of nondisclosure agreements, such as SF 312, Classified Information Nondisclosure Agreement,	**Records maintained in the individual's official personnel folder.**	Apply the disposition for the official personnel folder.	

Item	Records Description		Disposition Instruction	Disposition Authority
121	signed by civilian and military personnel with access to information that is classified under standards put forth by executive orders governing security classification.	**Records maintained separately from the individual's official personnel folder.** **Legal citations:** ICD 703, Protection of Classified National Intelligence; 32 CFR 2001.80(d)(2)(vii).	**Temporary**. Destroy when 50 years old.	DAA-GRS-2015-0002-0003
130	**Personally identifiable information extracts.** System-generated or hardcopy print-outs generated for business purposes that contain Personally Identifiable Information. **Legal citation**: OMB M-07-16 (May 22, 2007), Attachment 1, Section C, bullet "Log and Verify."		**Temporary**. Destroy when 90 days old or no longer needed pursuant to supervisory authorization, whichever is appropriate.	DAA-GRS-2013-0007-0012
140	**Personally identifiable information extract logs.** Logs that track the use of PII extracts by authorized users, containing some or all of: date and time of extract, name and component of information system from which data is extracted, user extracting data, data elements involved, business purpose for which the data will be used, length of time extracted information will be used. Also includes (if appropriate): justification and supervisory authorization for retaining extract longer than 90 days, and anticipated disposition date.		**Temporary**. Destroy when business use ceases.	DAA-GRS-2013-0007-0013
150	**Privacy Act System of Records Notices (SORNs).** Agency copy of notices about the existence and character of systems of records, documenting publication in the Federal Register when the agency establishes or revises the system, per the Privacy Act of 1974 [5 U.S.C. 552a(e)(4) and 5 U.S.C. 552a(e)(11)], as amended. Also significant material documenting SORN formulation, other than Privacy Impact Assessment records (see item 161).		**Temporary**. Destroy 2 years after supersession by a revised SORN or after system ceases operation, but longer retention is authorized if required for business use.	DAA-GRS-2016-0003-0002
160	**Records analyzing Personally Identifiable Information (PII).** Records documenting whether certain privacy and data security laws, regulations, and agency policies are required; how the agency collects, uses, shares, and maintains PII; and incorporation of privacy protections into	**Records of Privacy Threshold Analyses (PTAs) and Initial Privacy Assessments (IPAs).** Records of research on whether an agency should conduct a Privacy Impact Assessment (PIA).	**Temporary**. Destroy 3 years after associated PIA is published or determination that PIA is unnecessary, but longer retention is authorized if required for business use.	DAA-GRS-2016-0003-0003

Item	Records Description		Disposition Instruction	Disposition Authority
161	records systems as required by the E-Government Act of 2002 (Public Law 107-347, section 208), the Privacy Act of 1974 (5 U.S.C. 552a), and other applicable privacy laws, regulations, and agency policies. Includes significant background material documenting formulation of final products.	**Records of Privacy Impact Assessments (PIAs).**	**Temporary**. Destroy 3 years after a superseding PIA is published, after system ceases operation, or (if PIA concerns a website) after website is no longer available to the public, as appropriate. Longer retention is authorized if required for business use.	DAA-GRS-2016-0003-0004
170	**Computer matching program notices and agreements.** Agency copy of notices of intent to share data in systems of records with other Federal, state, or local government agencies via computer matching programs, and related records documenting publication of notice in the Federal Register per the Privacy Act of 1974 [5 U.S.C. 552a(e)(12)], as amended. Also agreements between agencies, commonly referred to as Computer Matching Agreements, prepared in accordance with Office of Management and Budget Final Guidance. Includes documentation of Data Integrity Board (DIB) review and approval of matching programs and agreements, and significant background material documenting formulation of notices and agreements.		**Temporary**. Destroy upon supersession by a revised notice or agreement, or 2 years after matching program ceases operation, but longer retention is authorized if required for business use.	DAA-GRS-2016-0003-0005
180	**Virtual public access library records.** Records published by an agency on line to fulfill the requirement in 5 U.S.C. 552(a)(2)(A) through 5 U.S.C. 552(a)(2)(D) and 5 U.S.C. 552(g)(1) through 5 U.S.C. 552(g)(3) that agencies must make those records available for public inspection and copying. Includes: • final concurring and dissenting opinions and orders agencies issue when adjudicating cases • statements of policy and interpretations the agency adopts but does not publish in the *Federal Register* • administrative staff manuals and instructions to staff that affect a member of the public • copies of records requested under the Freedom of Information Act (FOIA) which, because of the nature of their subject matter, the agency determines are, or are likely to become, the subject of subsequent requests for substantially the same records or which have been requested three or more times • indexes of agency major information systems		**Temporary**. Destroy when no longer needed.	DAA-GRS-2016-0008-0001

Item	Records Description	Disposition Instruction	Disposition Authority
	• descriptions of agency major information and record locator systems • handbooks for obtaining various types and categories of agency public information **Exclusion**: This item refers only to copies an agency publishes on line for public reference. The agency record copy of such material may be of permanent value and the agency must schedule it. Not media neutral. Applies to electronic records only.		
Controlled Unclassified Information (CUI) program records. **Exclusion:** Records of the Controlled Unclassified Information Executive Agent office at the National Archives (NARA must schedule these records separately).			
190	**CUI program implementation records.** Records of overall program management. Includes: • records documenting the process of planning agency policy and procedure • agency submissions to the CUI Executive Agent of authorities (laws, Federal regulations, or Government-wide policies containing safeguarding or dissemination controls) the agency proposes to include in the CUI Registry to designate unclassified information as CUI • agency submissions to the CUI Executive Agent of proposed laws, Federal regulations, or Government-wide policies that would establish, eliminate, or modify a category of CUI, or change information controls applicable to CUI • correspondence with CUI Executive Agent **Exclusion 1**: CUI directives and formal policy documents (agencies must schedule these separately). **Exclusion 2**: Records of CUI self-inspections (GRS 5.7, item 020 covers these). **Exclusion 3**: Records of annual program reports to the CUI Executive Agent (GRS 5.7, item 050 covers these).	**Temporary**. Destroy when 7 years old, but longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0005
191	**CUI information sharing agreements.** Agreements in which agencies agree to share CUI with non-executive branch entities (*e.g.*, state and local police) and foreign entities that agree to protect the CUI.	**Temporary**. Destroy 7 years after canceled or superseded, but longer retention is	DAA-GRS-2019-0001-0006

Item	Records Description		Disposition Instruction	Disposition Authority
	Exclusion: Contracts involving CUI and contractor access to CUI; GRS 1.1, item 010 covers contracts.		authorized if required for business use.	
192	**Records of waivers of CUI requirements.** Description of and rationale for each waiver, documentation of alternate steps the agency takes to ensure it sufficiently protects the CUI covered by the waiver, and records of the agency notifying authorized recipients and the public of the waiver.		**Temporary**. Destroy when waiver is rescinded, system is no longer in use, or all affected records are destroyed, as applicable, but longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0007
193	**Records of requests for decontrol and challenges to CUI designations.** Requests to decontrol CUI or challenging a CUI marking as incorrect (either improperly assigned or lacking), responses to requests, records of adjudication, and records of dispute resolution if adjudication is appealed.	**Records filed with the record-keeping copy of the CUI-marked records.**	Follow the disposition instructions approved for the records at issue.	
194		**Records filed separately from the record-keeping copy of the CUI-marked records.**	**Temporary.** Destroy 6 years after change in CUI status, but longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0008
195	**Records of CUI misuse.** Allegations of CUI misuse, records of internal investigations, communications with and reports of findings from the CUI Executive Agent, and records of corrective actions. **Exclusion**: If the agency assigns such investigations to its Inspector General (IG), the agency schedule for IG records covers the records created in the IG office.		**Temporary**. Destroy 5 years after completing the investigation or completing all corrective actions, whichever is later, but longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0009

EXHIBIT G

Declaration for Federal Employment*

(*This form may also be used to assess fitness for federal contract employment)

Form Approved:
OMB No. 3206-0182

Instructions

The information collected on this form is used to determine your acceptability for Federal and Federal contract employment and your enrollment status in the Government's Life Insurance program. You may be asked to complete this form at any time during the hiring process. Follow instructions that the agency provides. If you are selected, before you are appointed you will be asked to update your responses on this form and on other materials submitted during the application process and then to recertify that your answers are true.

All your answers must be truthful and complete. **A false statement on any part of this declaration or attached forms or sheets may be grounds for not hiring you, or for firing you after you begin work. Also, you may be punished by a fine or imprisonment (U.S. Code, title 18, section 1001).**

Either type your responses on this form or print clearly in dark ink. If you need additional space, attach letter-size sheets (8.5" X 11"). Include your name, Social Security Number, and item number on each sheet. We recommend that you keep a photocopy of your completed form for your records.

Privacy Act Statement

The Office of Personnel Management is authorized to request this information under sections 1302, 3301, 3304, 3328, and 8716 of title 5, U. S. Code. Section 1104 of title 5 allows the Office of Personnel Management to delegate personnel management functions to other Federal agencies. If necessary, and usually in conjunction with another form or forms, this form may be used in conducting an investigation to determine your suitability or your ability to hold a security clearance, and it may be disclosed to authorized officials making similar, subsequent determinations.

Your Social Security Number (SSN) is needed to keep our records accurate, because other people may have the same name and birth date. Public Law 104-134 (April 26, 1996) asks Federal agencies to use this number to help identify individuals in agency records. Giving us your SSN or any other information is voluntary. However, if you do not give us your SSN or any other information requested, we cannot process your application. Incomplete addresses and ZIP Codes may also slow processing.

ROUTINE USES: Any disclosure of this record or information in this record is in accordance with routine uses found in System Notice OPM/GOVT-1, General Personnel Records. This system allows disclosure of information to: training facilities; organizations deciding claims for retirement, insurance, unemployment, or health benefits; officials in litigation or administrative proceedings where the Government is a party; law enforcement agencies concerning a violation of law or regulation; Federal agencies for statistical reports and studies; officials of labor organizations recognized by law in connection with representation of employees; Federal agencies or other sources requesting information for Federal agencies in connection with hiring or retaining, security clearance, security or suitability investigations, classifying jobs, contracting, or issuing licenses, grants, or other benefits; public and private organizations, including news media, which grant or publicize employee recognitions and awards; the Merit Systems Protection Board, the Office of Special Counsel, the Equal Employment Opportunity Commission, the Federal Labor Relations Authority, the National Archives and Records Administration, and Congressional offices in connection with their official functions; prospective non-Federal employers concerning tenure of employment, civil service status, length of service, and the date and nature of action for separation as shown on the SF 50 (or authorized exception) of a specifically identified individual; requesting organizations or individuals concerning the home address and other relevant information on those who might have contracted an illness or been exposed to a health hazard; authorized Federal and non-Federal agencies for use in computer matching; spouses or dependent children asking whether the employee has changed from a self-and-family to a self-only health benefits enrollment; individuals working on a contract, service, grant, cooperative agreement, or job for the Federal government; non-agency members of an agency's performance or other panel; and agency-appointed representatives of employees concerning information issued to the employees about fitness-for-duty or agency-filed disability retirement procedures.

Public Burden Statement

Public burden reporting for this collection of information is estimated to vary from 5 to 30 minutes with an average of 15 minutes per response, including time for reviewing instructions, searching existing data sources, gathering the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden, to the U.S. Office of Personnel Management, Reports and Forms Manager (3206-0182), Washington, DC 20415-7900. The OMB number, 3206-0182, is valid. OPM may not collect this information, and you are not required to respond, unless this number is displayed.

Declaration for Federal Employment*

(*This form may also be used to assess fitness for federal contract employment)

Form Approved:
OMB No. 3206-0182

GENERAL INFORMATION

1. **FULL NAME** (Provide your full name. If you have only initials in your name, provide them and indicate "Initial only". If you do not have a middle name, indicate "No Middle Name". If you are a "Jr.," "Sr.," etc. enter this under Suffix. First, Middle, Last, Suffix)

♦

2. SOCIAL SECURITY NUMBER	3a. PLACE OF BIRTH (Include city and state or country)
♦	♦

3b. ARE YOU A U.S. CITIZEN?	4. DATE OF BIRTH (MM / DD / YYYY)
☐ YES ☐ NO (If "NO", provide country of citizenship) ♦	♦
5. OTHER NAMES EVER USED (For example, maiden name, nickname, etc)	**6. PHONE NUMBERS** (Include area codes)
♦	Day ♦
♦	Night ♦

Selective Service Registration

If you are a male born after December 31, 1959, and are at least 18 years of age, civil service employment law (5 U.S.C. 3328) requires that you must register with the Selective Service System, unless you meet certain exemptions.

7a. Are you a male born after December 31, 1959? ☐ YES ☐ NO (If "NO", proceed to 8.)

7b. Have you registered with the Selective Service System? ☐ YES (If "YES", proceed to 8.) ☐ NO (If "NO", proceed to 7c.)

7c. If "NO," describe your reason(s) in item 16.

Military Service

8. Have you ever served in the United States military? ☐ YES (If "YES", provide information below) ☐ NO

If you answered "YES," list the branch, dates, and type of discharge for all active duty.
If your only active duty was training in the Reserves or National Guard, answer "NO."

Branch	From (MM/DD/YYYY)	To (MM/DD/YYYY)	Type of Discharge

Background Information

For all questions, provide all additional requested information under item 16 or on attached sheets. The circumstances of each event you list will be considered. However, in most cases you can still be considered for Federal jobs.

For questions 9,10, and 11, your answers should include convictions resulting from a plea of *nolo contendere* (no contest), but omit (1) traffic fines of $300 or less, (2) any violation of law committed before your 16th birthday, (3) any violation of law committed before your 18th birthday if finally decided in juvenile court or under a Youth Offender law, (4) any conviction set aside under the Federal Youth Corrections Act or similar state law, and (5) any conviction for which the record was expunged under Federal or state law .

9. During the last 7 years, have you been convicted, been imprisoned, been on probation, or been on parole? (Includes felonies, firearms or explosives violations, misdemeanors, and all other offenses.) *If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved.* ☐ YES ☐ NO

10. Have you been convicted by a military court-martial in the past 7 years? *(If no military service, answer "NO.") If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the military authority or court involved.* ☐ YES ☐ NO

11. Are you currently under charges for any violation of law? *If "YES," use item 16 to provide the date, explanation of the violation, place of occurrence, and the name and address of the police department or court involved.* ☐ YES ☐ NO

12. During the last 5 years, have you been fired from any job for any reason, did you quit after being told that you would be fired, did you leave any job by mutual agreement because of specific problems, or were you debarred from Federal employment by the Office of Personnel Management or any other Federal agency? *If "YES," use item 16 to provide the date, an explanation of the problem, reason for leaving, and the employer's name and address.* ☐ YES ☐ NO

13. Are you delinquent on any Federal debt? (Includes delinquencies arising from Federal taxes, loans, overpayment of benefits, and other debts to the U.S. Government, plus defaults of Federally guaranteed or insured loans such as student and home mortgage loans.) *If "YES," use item 16 to provide the type, length, and amount of the delinquency or default, and steps that you are taking to correct the error or repay the debt.* ☐ YES ☐ NO

Declaration for Federal Employment*

(*This form may also be used to assess fitness for federal contract employment)

Form Approved:
OMB No. 3206-0182

Additional Questions

14. Do any of your relatives work for the agency or government organization to which you are submitting this form? (Include: father, mother, husband, wife, son, daughter, brother, sister, uncle, aunt, first cousin, nephew, niece, father-in-law,mother-in-law, son-in-law, daughter-in-law, brother-in-law, sister-in-law, stepfather, stepmother, stepson, stepdaughter, stepbrother, stepsister, half brother, and half sister.) *If "YES," use item 16 to provide the relative's name,relationship, and the department, agency, or branch of the Armed Forces for which your relative works.* ☐ YES ☐ NO

15. Do you receive, or have you ever applied for, retirement pay, pension, or other retired pay based on military, Federal civilian, or District of Columbia Government service? ☐ YES ☐ NO

Continuation Space / Agency Optional Questions

16. Provide details requested in items 7 through 15 and 18c in the space below or on attached sheets. Be sure to identify attached sheets with your name, Social Security Number, and item number, and to include ZIP Codes in all addresses. If any questions are printed below, please answer as instructed *(these questions are specific to your position and your agency is authorized to ask them).*

Certifications / Additional Questions

APPLICANT: If you are applying for a position and have not yet been selected, carefully review your answers on this form and any attached sheets. When this form and all attached materials are accurate, read item 17, and complete 17a.

APPOINTEE: If you are being appointed, carefully review your answers on this form and any attached sheets, including any other application materials that your agency has attached to this form. If any information requires correction to be accurate as of the date you are signing, make changes on this form or the attachments and/or provide updated information on additional sheets, initialing and dating all changes and additions. When this form and all attached materials are accurate, read item 17, complete 17b, read 18, and answer 18a, 18b, and 18c as appropriate.

17. **I certify** that, to the best of my knowledge and belief, all of the information on and attached to this Declaration for Federal Employment, including any attached application materials, is true, correct, complete, and made in good faith . **I understand that a false or fraudulent answer to any question or item on any part of this declaration or its attachments may be grounds for not hiring me, or for firing me after I begin work, and may be punishable by fine or imprisonment. I understand** that any information I give may be investigated for purposes of determining eligibility for Federal employment as allowed by law or Presidential order. **I consent** to the release of information about my ability and fitness for Federal employment by employers, schools, law enforcement agencies, and other individuals and organizations to investigators, personnel specialists, and other authorized employees or representatives of the Federal Government. **I understand** that for financial or lending institutions, medical institutions, hospitals, health care professionals, and some other sources of information, a separate specific release may be needed, and I may be contacted for such a release at a later date.

17a. Applicant's Signature: _____ (Sign in ink) Date _____

17b. Appointee's Signature: _____ (Sign in ink) Date _____

Appointing Officer:
Enter Date of Appointment or Conversion
MM / DD / YYYY

18. **Appointee (Only respond if you have been employed by the Federal Government before):** Your elections of life insurance during previous Federal employment may affect your eligibility for life insurance during your new appointment. These questions are asked to help your personnel office make a correct determination.

18a. When did you leave your last Federal job? DATE: MM / DD / YYYY

18b. When you worked for the Federal Government the last time, did you waive Basic Life Insurance or any type of optional life insurance? ☐ YES ☐ NO ☐ DO NOT KNOW

18c. If you answered "YES" to item 18b, did you later cancel the waiver(s)? If your answer to item 18c is "NO," use item 16 to identify the type(s) of insurance for which waivers were not canceled. ☐ YES ☐ NO ☐ DO NOT KNOW

EXHIBIT H

Standard Form 85P
Revised September 1995
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

Form approved:
OMB No. 3206-0191
NSN 7540-01-317-7372
85-1602

Questionnaire for Public Trust Positions

Follow instructions fully or we cannot process your form. Be sure to sign and date the certification statement on Page 7 and the release on Page 8. *If you have any questions,* call the office that gave you the form.

Purpose of this Form

The U.S. Government conducts background investigations and reinvestigations to establish that applicants or incumbents either employed by the Government or working for the Government under contract, are suitable for the job and/or eligible for a public trust or sensitive position. Information from this form is used primarily as the basis for this investigation. Complete this form only after a conditional offer of employment has been made.

Giving us the information we ask for is voluntary. However, we may not be able to complete your investigation, or complete it in a timely manner, if you don't give us each item of information we request. This may affect your placement or employment prospects.

Authority to Request this Information

The U.S. Government is authorized to ask for this information under Executive Orders 10450 and 10577, sections 3301 and 3302 of title 5, U.S. Code; and parts 5, 731, 732, and 736 of Title 5, Code of Federal Regulations.

Your Social Security number is needed to keep records accurate, because other people may have the same name and birth date. Executive Order 9397 also asks Federal agencies to use this number to help identify individuals in agency records.

The Investigative Process

Background investigations are conducted using your responses on this form and on your Declaration for Federal Employment (OF 306) to develop information to show whether you are reliable, trustworthy, of good conduct and character, and loyal to the United States. The information that you provide on this form is confirmed during the investigation. Your current employer must be contacted as part of the investigation, even if you have previously indicated on applications or other forms that you do not want this.

In addition to the questions on this form, inquiry also is made about a person's adherence to security requirements, honesty and integrity, vulnerability to exploitation or coercion, falsification, misrepresentation, and any other behavior, activities, or associations that tend to show the person is not reliable, trustworthy, or loyal.

Your Personal Interview

Some investigations will include an interview with you as a normal part of the investigative process. This provides you the opportunity to update, clarify, and explain information on your form more completely, which often helps to complete your investigation faster. It is important that the interview be conducted as soon as possible after you are contacted. Postponements will delay the processing of your investigation, and declining to be interviewed may result in your investigation being delayed or canceled.

You will be asked to bring identification with your picture on it, such as a valid State driver's license, to the interview. There are other documents you may be asked to bring to verify your identity as well. These include documentation of any legal name change, Social Security card, and/or birth certificate.

You may also be asked to bring documents about information you provided on the form or other matters requiring specific attention. These matters include alien registration, delinquent loans or taxes, bankruptcy, judgments, liens, or other financial obligations, agreements involving child custody or support, alimony or property settlements, arrests, convictions, probation, and/or parole.

Instructions for Completing this Form

1. Follow the instructions given to you by the person who gave you the form and any other clarifying instructions furnished by that person to assist you in completion of the form. Find out how many copies of the form you are to turn in. You must sign and date, in black ink, the original and each copy you submit.

2. Type or legibly print your answers in black ink (if your form is not legible, it will not be accepted). You may also be asked to submit your form in an approved electronic format.

3. All questions on this form must be answered. If no response is necessary or applicable, indicate this on the form (for example, enter "None" or "N/A"). If you find that you cannot report an exact date, approximate or estimate the date to the best of your ability and indicate this by marking "APPROX." or "EST."

4. Any changes that you make to this form after you sign it must be initialed and dated by you. Under certain limited circumstances, agencies may modify the form consistent with your intent.

5. You must use the State codes (abbreviations) listed on the back of this page when you fill out this form. Do not abbreviate the names of cities or foreign countries.

6. The 5-digit postal ZIP codes are needed to speed the processing of your investigation. The office that provided the form will assist you in completing the ZIP codes.

7. All telephone numbers must include area codes.

8. All dates provided on this form must be in Month/Day/Year or Month/Year format. Use numbers (1-12) to indicate months. For example, June 10, 1978, should be shown as 6/10/78.

9. Whenever "City (Country)" is shown in an address block, also provide in that block the name of the country when the address is outside the United States.

10. If you need additional space to list your residences or employments/self-employments/unemployments or education, you should use a continuation sheet, SF 86A. If additional space is needed to answer other items, use a blank piece of paper. Each blank piece of paper you use must contain **your name and Social Security Number at the top of the page.**

Final Determination on Your Eligibility

Final determination on your eligibility for a public trust or sensitive position and your being granted a security clearance is the responsibility of the Office of Personnel Management or the Federal agency that requested your investigation. You may be provided the opportunity personally to explain, refute, or clarify any information before a final decision is made.

Penalties for Inaccurate or False Statements

The U.S. Criminal Code (title 18, section 1001) provides that knowingly falsifying or concealing a material fact is a felony which may result in fines of up to $10,000, and/or 5 years imprisonment, or both. In addition, Federal agencies generally fire, do not grant a security clearance, or disqualify individuals who have materially and deliberately falsified these forms, and this remains a part of the permanent record for future placements. Because the position for which you are being considered is one of public trust or is sensitive, your trustworthiness is a very important consideration in deciding your suitability for placement or retention in the position.

Your prospects of placement are better if you answer all questions truthfully and completely. You will have adequate opportunity to explain any information you give us on the form and to make your comments part of the record.

Disclosure of Information

The information you give us is for the purpose of investigating you for a position; we will protect it from unauthorized disclosure. The collection, maintenance, and disclosure of background investigative information is governed by the Privacy Act. The agency which requested the investigation and the agency which conducted the investigation have published notices in the Federal Register describing the system of records in which your records will be maintained. You may obtain copies of the relevant notices from the person who gave you this form. The information on this form, and information we collect during an investigation may be disclosed without your consent as permitted by the Privacy Act (5 USC 552a(b)) and as follows:

PRIVACY ACT ROUTINE USES

1. To the Department of Justice when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

2. To a court or adjudicative body in a proceeding when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (d) the United States Government is a party to litigation or has interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

3. Except as noted in Question 21, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute, particular program statute, regulation, rule, or order issued pursuant thereto, the relevant records may be disclosed to the appropriate Federal, foreign, State, local, tribal, or other public authority responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order.

4. To any source or potential source from which information is requested in the course of an investigation concerning the hiring or retention of an employee or other personnel action, or the issuing or retention of a security clearance, contract, grant, license, or other benefit, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

5. To a Federal, State, local, foreign, tribal, or other public authority the fact that this system of records contains information relevant to the retention of an employee, or the retention of a security clearance, contract, license, grant, or other benefit. The other agency or licensing organization may then make a request supported by written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action.

6. To contractors, grantees, experts, consultants, or volunteers when necessary to perform a function or service related to this record for which they have been engaged. Such recipients shall be required to comply with the Privacy Act of 1974, as amended.

7. To the news media or the general public, factual information the disclosure of which would be in the public interest and which would not constitute an unwarranted invasion of personal privacy.

8. To a Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.

9. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.

10. To the National Archives and Records Administration for records management inspections conducted under 44 USC 2904 and 2906.

11. To the Office of Management and Budget when necessary to the review of private relief legislation.

STATE CODES (ABBREVIATIONS)

Alabama	AL	Hawaii	HI	Massachusetts	MA	New Mexico	NM	South Dakota	SD
Alaska	AK	Idaho	ID	Michigan	MI	New York	NY	Tennessee	TN
Arizona	AZ	Illinois	IL	Minnesota	MN	North Carolina	NC	Texas	TX
Arkansas	AR	Indiana	IN	Mississippi	MS	North Dakota	ND	Utah	UT
California	CA	Iowa	IA	Missouri	MO	Ohio	OH	Vermont	VT
Colorado	CO	Kansas	KS	Montana	MT	Oklahoma	OK	Virginia	VA
Connecticut	CT	Kentucky	KY	Nebraska	NE	Oregon	OR	Washington	WA
Delaware	DE	Louisiana	LA	Nevada	NV	Pennsylvania	PA	West Virginia	WV
Florida	FL	Maine	ME	New Hampshire	NH	Rhode Island	RI	Wisconsin	WI
Georgia	GA	Maryland	MD	New Jersey	NJ	South Carolina	SC	Wyoming	WY
American Samoa	AS	District of Columbia	DC	Guam	GU	Northern Marianas	CM	Puerto Rico	PR
Trust Territory	TT	Virgin Islands	VI						

PUBLIC BURDEN INFORMATION

Public burden reporting for this collection of information is estimated to average 60 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Reports and Forms Management Officer, U.S. Office of Personnel Management, 1900 E Street, N.W., Room CHP-500, Washington, D.C. 20415. Do not send your completed form to this address.

Standard Form 85P (EG)
Revised September 1995
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR PUBLIC TRUST POSITIONS

Form approved:
OMB No. 3206-0191
NSN 7540-01-317-7372
85-1602

OPM USE ONLY — Codes — Case Number

Agency Use Only ***(Complete items A through P using instructions provided by USOPM)***

A Type of Investigation	B Extra Coverage	C Sensitivity/ Risk Level	D Compu/ ADP	E Nature of Action Code	F Date of Action (Month / Day / Year)

G Geographic Location	H Position Code	I Position Title

J SON	K Location of Official Personnel Folder	Other Address	ZIP Code
	☐ None ☐ NPRC ☐ At SON		

L SOI	M Location of Security Folder	Other Address	ZIP Code
	☐ None ☐ At SOI ☐ NPI		

N OPAC-ALC Number	O Accounting Data and/or Agency Case Number

P Requesting Official — Name and Title	Signature	Telephone Number ( )	Date
		( )	

Persons completing this form should begin with the questions below.

1 FULL NAME • If you have only initials in your name, use them and state (IO). • If you have no middle name, enter "NMN". - If you are a "Jr.," "Sr.," "II," etc., enter this in the box after your middle name.

2 DATE OF BIRTH

Last Name	First Name	Middle Name	Jr., II, etc.	Month	Day	Year

3 PLACE OF BIRTH - Use the two letter code for the State.

City	County	State	Country *(if not in the United States)*

4 SOCIAL SECURITY NUMBER

5 OTHER NAMES USED

	Name	Month/Year	Month/Year
#1			To
#2			To
#3			To
#4			To

6 OTHER IDENTIFYING INFORMATION

Height *(feet and inches)*	Weight *(pounds)*	Hair Color	Eye Color	Sex *(Mark one box)*
				☐ Female ☐ Male

7 TELEPHONE NUMBERS

Work *(include Area Code and extension)*	Home *(include Area Code)*
☐ Day ☐ Night ( )	☐ Day ☐ Night ( )

8 CITIZENSHIP

a Mark the box at the right that reflects your current citizenship status, and follow its instructions.

- ☐ I am a U.S. citizen or national by birth in the U.S. or U.S. territory/possession. *Answer items b and d.*
- ☐ I am a U.S. citizen, but I was NOT born in the U.S. *Answer items b, c and d.*
- ☐ I am not a U.S. citizen. *Answer items b and e.*

b Your Mother's Maiden Name

c UNITED STATES CITIZENSHIP If you are a U.S. Citizen, but were not born in the U.S., provide information about one or more of the following proofs of your citizenship.

Naturalization Certificate *(Where were you naturalized?)*

Court	City	State	Certificate Number	Month/Day/Year Issued

Citizenship Certificate *(Where was the certificate issued?)*

City	State	Certificate Number	Month/Day/Year Issued

State Department Form 240 - Report of Birth Abroad of a Citizen of the United States

Give the date the form was prepared and give an explanation if needed.	Month/Day/Year	Explanation

U.S. Passport

This may be either a current or previous U.S. Passport	Passport Number	Month/Day/Year Issued

d DUAL CITIZENSHIP If you are *(or were)* a dual citizen of the United States and another country, provide the name of that country in the space to the right. — Country

e ALIEN If you are an alien, provide the following information:

Place You Entered the United States:	City	State	Date You Entered U.S. Month	Day	Year	Alien Registration Number	Country(ies) of Citizenship

9 WHERE YOU HAVE LIVED

List the places where you have lived, beginning with the most recent (#1) and working back 7 years. All periods must be accounted for in your list. Be sure to indicate the actual physical location of your residence: do not use a post office box as an address, do not list a permanent address when you were actually living at a school address, etc. Be sure to specify your location as closely as possible: for example, do not list only your base or ship, list your barracks number or home port. You may omit temporary military duty locations under 90 days (list your permanent address instead), and you should use your APO/FPO address if you lived overseas.

For any address in the last 5 years, list a person who knew you at that address, and who preferably still lives in that area (do not list people for residences completely outside this 5-year period, and do not list your spouse, former spouses, or other relatives). Also for addresses in the last 5 years, if the address is "General Delivery," a Rural or Star Route, or may be difficult to locate, provide directions for locating the residence on an attached continuation sheet.

#1	Month/Year To Present	Month/Year	Street Address	Apt. #	City (Country)		State	ZIP Code
Name of Person Who Knows You	Street Address	Apt. #	City (Country)	State	ZIP Code	Telephone Number ( )		
#2	Month/Year To	Month/Year	Street Address	Apt. #	City (Country)		State	ZIP Code
Name of Person Who Knew You	Street Address	Apt. #	City (Country)	State	ZIP Code	Telephone Number ( )		
#3	Month/Year To	Month/Year	Street Address	Apt. #	City (Country)		State	ZIP Code
Name of Person Who Knew You	Street Address	Apt. #	City (Country)	State	ZIP Code	Telephone Number ( )		
#4	Month/Year To	Month/Year	Street Address	Apt. #	City (Country)		State	ZIP Code
Name of Person Who Knew You	Street Address	Apt. #	City (Country)	State	ZIP Code	Telephone Number ( )		
#5	Month/Year To	Month/Year	Street Address	Apt. #	City (Country)		State	ZIP Code
Name of Person Who Knew You	Street Address	Apt. #	City (Country)	State	ZIP Code	Telephone Number ( )		

10 WHERE YOU WENT TO SCHOOL

List the schools you have attended, beyond Junior High School**, beginning with the most recent (#1) and working back 7 years.** List **all** College or University degrees and the dates they were received. If all of your education occurred more than 7 years ago, list your most recent education beyond high school, no matter when that education occurred.

- Use one of the following codes in the "Code" block:

  1 - High School **2 -** College/University/Military College **3 -** Vocational/Technical/Trade School

- For schools you attended in the past 3 years, list a person who knew you at school (an instructor, student, etc.). Do not list people for education completely outside this 3-year period.

- For correspondence schools and extension classes, provide the address where the records are maintained.

#1	Month/Year To	Month/Year	Code	Name of School	Degree/Diploma/Other		Month/Year Awarded	
Street Address and City (Country) of School						State	ZIP Code	
Name of Person Who Knew You	Street Address	Apt. #	City (Country)	State	ZIP Code	Telephone Number ( )		
#2	Month/Year To	Month/Year	Code	Name of School	Degree/Diploma/Other		Month/Year Awarded	
Street Address and City (Country) of School						State	ZIP Code	
Name of Person Who Knew You	Street Address	Apt. #	City (Country)	State	ZIP Code	Telephone Number ( )		
#3	Month/Year To	Month/Year	Code	Name of School	Degree/Diploma/Other		Month/Year Awarded	
Street Address and City (Country) of School						State	ZIP Code	
Name of Person Who Knew You	Street Address	Apt. #	City (Country)	State	ZIP Code	Telephone Number ( )		

Enter your Social Security Number before going to the next page →

11 YOUR EMPLOYMENT ACTIVITIES

List your employment activities, beginning with the present (#1) and working back 7 years. You should list all full-time work, part-time work, military service, temporary military duty locations over 90 days, self-employment, other paid work, and all periods of unemployment. The entire 7-year period must be accounted for without breaks, but you need not list employments before your 16th birthday.

- **Code.** Use one of the codes listed below to identify the type of employment:
  - **1** - Active military duty stations
  - **2** - National Guard/Reserve
  - **3** - U.S.P.H.S. Commissioned Corps
  - **4** - Other Federal employment
  - **5** - State Government (Non-Federal employment)
  - **6** - Self-employment (Include business and/or name of person who can verify)
  - **7** - Unemployment (Include name of person who can verify)
  - **8** - Federal Contractor (List Contractor, not Federal agency)
  - **9** - Other
- **Employer/Verifier Name.** List the business name of your employer or the name of the person who can verify your self-employment or unemployment in this block. If military service is being listed, include your duty location or home port here as well as your branch of service. You should provide separate listings to reflect changes in your military duty locations or home ports.
- **Previous Periods of Activity.** Complete these lines if you worked for an employer on more than one occasion at the same location. After entering the most recent period of employment in the initial numbered block, provide previous periods of employment at the same location on the additional lines provided. For example, if you worked at XY Plumbing in Denver, CO, during 3 separate periods of time, you would enter dates and information concerning the most recent period of employment first, and provide dates, position titles, and supervisors for the two previous periods of employment on the lines below that information.

Month/Year Month/Year	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
#1 To Present			

Employer's/Verifier's Street Address	City (Country)	State	ZIP Code	Telephone Number
				( )
Street Address of Job Location (if different than Employer's Address)	City (Country)	State	ZIP Code	Telephone Number
				( )
Supervisor's Name & Street Address (if different than Job Location)	City (Country)	State	ZIP Code	Telephone Number
				( )

PREVIOUS PERIODS OF ACTIVITY *(Block #1)*	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor

Month/Year Month/Year	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
#2 To			

Employer's/Verifier's Street Address	City (Country)	State	ZIP Code	Telephone Number
				( )
Street Address of Job Location (if different than Employer's Address)	City (Country)	State	ZIP Code	Telephone Number
				( )
Supervisor's Name & Street Address (if different than Job Location)	City (Country)	State	ZIP Code	Telephone Number
				( )

PREVIOUS PERIODS OF ACTIVITY *(Block #2)*	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor

Month/Year Month/Year	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
#3 To			

Employer's/Verifier's Street Address	City (Country)	State	ZIP Code	Telephone Number
				( )
Street Address of Job Location (if different than Employer's Address)	City (Country)	State	ZIP Code	Telephone Number
				( )
Supervisor's Name & Street Address (if different than Job Location)	City (Country)	State	ZIP Code	Telephone Number
				( )

PREVIOUS PERIODS OF ACTIVITY *(Block #3)*	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor

Enter your Social Security Number before going to the next page →

YOUR EMPLOYMENT ACTIVITIES *(CONTINUED)*

#4	Month/Year To	Month/Year	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
Employer's/Verifier's Street Address			City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)			City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)			City (Country)	State	ZIP Code	Telephone Number ( )

PREVIOUS PERIODS OF ACTIVITY *(Block #4)*	Month/Year To	Month/Year	Position Title	Supervisor
	Month/Year To	Month/Year	Position Title	Supervisor
	Month/Year To	Month/Year	Position Title	Supervisor

#5	Month/Year To	Month/Year	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
Employer's/Verifier's Street Address			City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)			City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)			City (Country)	State	ZIP Code	Telephone Number ( )

PREVIOUS PERIODS OF ACTIVITY *(Block #5)*	Month/Year To	Month/Year	Position Title	Supervisor
	Month/Year To	Month/Year	Position Title	Supervisor
	Month/Year To	Month/Year	Position Title	Supervisor

#6	Month/Year To	Month/Year	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
Employer's/Verifier's Street Address			City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)			City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)			City (Country)	State	ZIP Code	Telephone Number ( )

PREVIOUS PERIODS OF ACTIVITY *(Block #6)*	Month/Year To	Month/Year	Position Title	Supervisor
	Month/Year To	Month/Year	Position Title	Supervisor
	Month/Year To	Month/Year	Position Title	Supervisor

12 **YOUR EMPLOYMENT RECORD**

Has any of the following happened to you in the last 7 years? If "Yes," begin with the most recent occurrence and go backward, providing date fired, quit, or left, and other information requested.	Yes	No

Use the following codes and explain the reason your employment was ended:

1 - Fired from a job

2 - Quit a job after being told you'd be fired

3 - Left a job by mutual agreement following allegations of misconduct

4 - Left a job by mutual agreement following allegations of unsatisfactory performance

5 - Left a job for other reasons under unfavorable circumstances

Month/Year	Code	Specify Reason	Employer's Name and Address *(Include city/Country if outside U.S.)*	State	ZIP Code

Enter your Social Security Number before going to the next page →

13 PEOPLE WHO KNOW YOU well

List three people who know you well and live in the United States. They should be good friends, peers, colleagues, college roommates, etc., whose combined association with you covers as well as possible the last 7 years. Do not list your spouse, former spouses, or other relatives, and try not to list anyone who is listed elsewhere on this form.

Name	Dates Known Month/Year To Month/Year	Telephone Number Day / Night ( )
#1		
Home or Work Address	City (Country)	State / ZIP Code

Name	Dates Known Month/Year To Month/Year	Telephone Number Day / Night ( )
#2		
Home or Work Address	City (Country)	State / ZIP Code

Name	Dates Known Month/Year To Month/Year	Telephone Number Day / Night ( )
#3		
Home or Work Address	City (Country)	State / ZIP Code

14 YOUR MARITAL STATUS

Mark one of the following boxes to show your current marital status:

☐ **1** - Never married *(go to question 15)*	☐ **3** - Separated	☐ **5** - Divorced
☐ **2** - Married	☐ **4** - Legally Separated	☐ **6** - Widowed

Current Spouse Complete the following about your current spouse.

Full Name	Date of Birth *(Mo./Day/Yr.)*	Place of Birth *(Include country if outside the U.S.)*	Social Security Number

Other Names Used *(Specify maiden name, names by other marriages, etc., and show dates used for each name)*

Country of Citizenship	Date Married *(Mo./Day/Yr.)*	Place Married *(Include country if outside the U.S.)*	State

If Separated, Date of Separation *(Mo./Day/Yr.)*	If Legally Separated, Where is the Record Located? City *(Country)*	State

Address of Current Spouse *(Street, city, and country if outside the U.S.)*	State	ZIP Code

15 YOUR RELATIVES

Give the full name, correct code, and other requested information for each of your relatives, living or dead, specified below.

1 - Mother *(first)* **2** - Father *(second)* **3** - Stepmother **4** - Stepfather **5** - Foster Parent **6** - Child *(adopted also)* **7** - Stepchild

	Full Name *(If deceased, check box on the left before entering name)*	Code	Date of Birth Month/Day/Year	Country of Birth	Country(ies) of Citizenship	Current Street Address and City *(country)* of Living Relatives	State
☐		**1**					
☐		**2**					
☐							
☐							
☐							
☐							
☐							
☐							
☐							
☐							
☐							

Enter your Social Security Number before going to the next page →

16 YOUR MILITARY HISTORY

		Yes	No
a	Have you served in the United States military?		
b	Have you served in the United States Merchant Marine?		

List all of your military service below, including service in Reserve, National Guard, and U.S. Merchant Marine. Start with the most recent period of service (#1) and work backward. If you had a break in service, each separate period should be listed.

- **Code.** Use one of the codes listed below to identify your branch of service:

1 - Air Force **2** - Army **3** - Navy **4** - Marine Corps **5** - Coast Guard **6** - Merchant Marine **7** - National Guard

- **O/E.** Mark "O" block for Officer or "E" block for Enlisted.

- **Status.** "X" the appropriate block for the status of your service during the time that you served. If your service was in the National Guard, do not use an "X": use the two-letter code for the state to mark the block.

- **Country.** If your service was with other than the U.S. Armed Forces, identify the country for which you served.

Month/Year To Month/Year	Code	Service/Certificate No.	O	E	Status: Active	Status: Active Reserve	Status: Inactive Reserve	Status: National Guard *(State)*	Country
To									
To									

17 YOUR SELECTIVE SERVICE RECORD

		Yes	No
a	Are you a male born after December 31, 1959? If "**No**," go to **18**. If "**Yes**," go to b.		
b	Have you registered with the Selective Service System? If "Yes," provide your registration number. If "**No**," show the reason for your legal exemption below.		

Registration Number	Legal Exemption Explanation

18 YOUR INVESTIGATIONS RECORD

		Yes	No
a	Has the United States Government ever investigated your background and/or granted you a security clearance? If "**Yes**," use the codes that follow to provide the requested information below. If "**Yes**," but you can't recall the investigating agency and/or the security clearance received, enter "**Other**" agency code or clearance code, as appropriate, and "**Don't know**" or "**Don't recall**" under the "**Other Agency**" heading, below. If your response is "**No**," or you don't know or can't recall if you were investigated and cleared, check the "**No**" box.		

Codes for Investigating Agency
1 - Defense Department **4** - FBI
2 - State Department **5** - Treasury Department
3 - Office of Personnel Management **6** - Other *(Specify)*

Codes for Security Clearance Received
0 - Not Required **3** - Top Secret **6** - L
1 - Confidential **4** - Sensitive Compartmented Information **7** - Other
2 - Secret **5** - Q

Month/Year	Agency Code	Other Agency	Clearance Code	Month/Year	Agency Code	Other Agency	Clearance Code

		Yes	No
b	To your knowledge, have you ever had a clearance or access authorization denied, suspended, or revoked, or have you ever been debarred from government employment? If "**Yes**," give date of action and agency. **Note:** An administrative downgrade or termination of a security clearance is not a revocation.		

Month/Year	Department or Agency Taking Action	Month/Year	Department or Agency Taking Action

19 FOREIGN COUNTRIES YOU HAVE VISITED

List foreign countries you have visited, except on travel under official Government orders, beginning with the most current (#1) and working back 7 years. (Travel as a dependent or contractor must be listed.)

- Use one of these codes to indicate the purpose of your visit: **1** - Business **2** - Pleasure **3** - Education **4** - Other

- Include short trips to Canada or Mexico. If you have lived near a border and have made short (one day or less) trips to the neighboring country, you do not need to list each trip. Instead, provide the time period, the code, the country, and a note ("Many Short Trips").

- Do not repeat travel covered in items 9, 10, or 11.

	Month/Year To Month/Year	Code	Country		Month/Year To Month/Year	Code	Country
#1	To			**#5**	To		
#2	To			**#6**	To		
#3	To			**#7**	To		
#4	To			**#8**	To		

Enter your Social Security Number before going to the next page →

20 YOUR POLICE RECORD *(Do not include anything that happened before your 16th birthday.)*

Yes	No

In the last 7 years, have you been arrested for, charged with, or convicted of any offense(s)? (Leave out traffic fines of less than $150.)

If you answered "Yes," explain your answer(s) in the space provided.

Month/Year	Offense	Action Taken	Law Enforcement Authority or Court *(City and county/country if outside the U.S.)*	State	ZIP Code

21 ILLEGAL DRUGS

Yes	No

The following questions pertain to the illegal use of drugs or drug activity. You are required to answer the questions fully and truthfully, and your failure to do so could be grounds for an adverse employment decision or action against you, but neither your truthful responses nor information derived from your responses will be used as evidence against you in any subsequent criminal proceeding.

a In the last year, have you illegally used any controlled substance, for example, marijuana, cocaine, crack cocaine, hashish, narcotics (opium, morphine, codeine, heroin, etc.), amphetamines, depressants (barbiturates, methaqualone, tranquilizers, etc.), hallucinogenics (LSD, PCP, etc.), or prescription drugs?

b In the last 7 years, have you been involved in the illegal purchase, manufacture, trafficking, production, transfer, shipping, receiving, or sale of any narcotic, depressant, stimulant, hallucinogen, or cannabis, for your own intended profit or that of another?

If you answered "Yes" to "a" above, provide information relating to the types of substance(s), the nature of the activity, and any other details relating to your involvement with illegal drugs. Include any treatment or counseling received.

Month/Year To Month/Year	Controlled Substance/Prescription Drug Used	Number of Times Used
To		
To		
To		

22 YOUR FINANCIAL RECORD

Yes	No

a In the last 7 years, have you, or a company over which you exercised some control, filed for bankruptcy, been declared bankrupt, been subject to a tax lien, or had legal judgment rendered against you for a debt? If you answered "Yes," provide date of initial action and other information requested below.

Month/Year	Type of Action	Name Action Occurred Under	Name/Address of Court or Agency Handling Case	State	ZIP Code

b Are you now over 180 days delinquent on any loan or financial obligation? Include loans or obligations funded or guaranteed by the Federal Government.

Yes	No

If you answered "**Yes**," provide the information requested below:

Month/Year	Type of Loan or Obligation and Account #	Name/Address of Creditor or Obligee	State	ZIP Code

After completing this form and any attachments, you should review your answers to all questions to make sure the form is complete and accurate, and then sign and date the following certification and sign and date the release on Page 8.

Certification That My Answers Are True

My statements on this form, and any attachments to it, are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both. (See section 1001 of title 18, United States Code).

Signature *(Sign in ink)* | Date

Enter your Social Security Number before going to the next page →

Standard Form 85P
Revised September 1995
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

Form approved:
OMB No. 3206-0191
NSN 7540-01-317-7372
85-1602

UNITED STATES OF AMERICA

AUTHORIZATION FOR RELEASE OF INFORMATION

Carefully read this authorization to release information about you, then sign and date it in ink.

I Authorize any investigator, special agent, or other duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain any information relating to my activities from individuals, schools, residential management agents, employers, criminal justice agencies, credit bureaus, consumer reporting agencies, collection agencies, retail business establishments, or other sources of information. This information may include, but is not limited to, my academic, residential, achievement, performance, attendance, disciplinary, employment history, criminal history record information, and financial and credit information. I authorize the Federal agency conducting my investigation to disclose the record of my background investigation to the requesting agency for the purpose of making a determination of suitability or eligibility for a security clearance.

I Understand that, for financial or lending institutions, medical institutions, hospitals, health care professionals, and other sources of information, a separate specific release will be needed, and I may be contacted for such a release at a later date. Where a separate release is requested for information relating to mental health treatment or counseling, the release will contain a list of the specific questions, relevant to the job description, which the doctor or therapist will be asked.

I Further Authorize any investigator, special agent, or other duly accredited representative of the U.S. Office of Personnel Management, the Federal Bureau of Investigation, the Department of Defense, the Defense Investigative Service, and any other authorized Federal agency, to request criminal record information about me from criminal justice agencies for the purpose of determining my eligibility for assignment to, or retention in a sensitive National Security position, in accordance with 5 U.S.C. 9101. I understand that I may request a copy of such records as may be available to me under the law.

I Authorize custodians of records and other sources of information pertaining to me to release such information upon request of the investigator, special agent, or other duly accredited representative of any Federal agency authorized above regardless of any previous agreement to the contrary.

I Understand that the information released by records custodians and sources of information is for official use by the Federal Government only for the purposes provided in this Standard Form 85P, and that it may be redisclosed by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for five (5) years from the date signed or upon the termination of my affiliation with the Federal Government, whichever is sooner.

Signature *(Sign in ink)*	Full Name *(Type or Print Legibly)*		Date Signed
Other Names Used			Social Security Number
Current Address *(Street, City)*	State	ZIP Code	Home Telephone Number *(Include Area Code)* ( )

Standard Form 85P
Revised September 1995
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

Form approved:
OMB No. 3206-0191
NSN 7540-01-317-7372
85-1602

UNITED STATES OF AMERICA

AUTHORIZATION FOR RELEASE OF MEDICAL INFORMATION

Carefully read this authorization to release information about you, then sign and date it in black ink.

Instructions for Completing this Release

This is a release for the investigator to ask your health practitioner(s) the three questions below concerning your mental health consultations. Your signature will allow the practitioner(s) to answer only these questions.

I am seeking assignment to or retention in a position of public trust with the Federal Government as a(n)

_____

(Investigator instructed to write in position title.)

As part of the investigative process, **I hereby authorize** the investigator, special agent, or duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain the following information relating to my mental health consultations:

Does the person under investigation have a condition or treatment that could impair his/her judgment or reliability?

If so, please describe the nature of the condition and the extent and duration of the impairment or treatment.

What is the prognosis?

I understand that the information released pursuant to this release is for use by the Federal Government only for purposes provided in the Standard Form 85P and that it may be redisclosed by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for 1 year from the date signed or upon termination of my affiliation with the Federal Government, whichever is sooner.

Signature *(Sign in ink)*	Full Name *(Type or Print Legibly)*		Date Signed
Other Names Used			Social Security Number
Current Address *(Street, City)*	State	ZIP Code	Home Telephone Number *(Include Area Code)* ( )

EXHIBIT I

APPLICANT
* See Privacy Act Notice on Back

FD-258 (Rev. 5-15-17) 1110-0046

LEAVE BLANK

TYPE OR PRINT ALL INFORMATION IN BLACK

LAST NAME NAM | FIRST NAME | MIDDLE NAME

FBI LEAVE BLANK

SIGNATURE OF PERSON FINGERPRINTED

ALIASES AKA

O
R
I

RESIDENCE OF PERSON FINGERPRINTED

DATE OF BIRTH DOB
Month Day Year

CITIZENSHIP CTZ | SEX | RACE | HGT. | WGT. | EYES | HAIR | PLACE OF BIRTH POB

DATE | SIGNATURE OF OFFICIAL TAKING FINGERPRINTS

YOUR NO. OCA

LEAVE BLANK

EMPLOYER AND ADDRESS

UNIVERSAL CONTROL NO. UCN

CLASS _____

ARMED FORCES NO. MNU

REF. _____

REASON FINGERPRINTED

SOCIAL SECURITY NO. SOC

MISCELLANEOUS NO. MNU

1. R. THUMB	2. R. INDEX	3. R. MIDDLE	4. R. RING	5. R. LITTLE
6. L. THUMB	7. L. INDEX	8. L. MIDDLE	9. L. RING	10. L. LITTLE

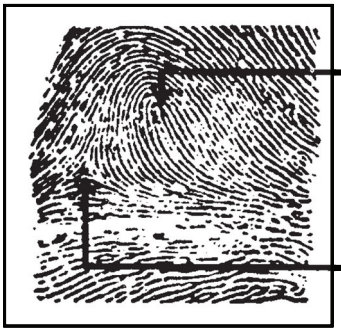
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY | L. THUMB | R. THUMB | RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY

1110-0046

FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE
CJIS DIVISION/CLARKSBURG, WV 26306

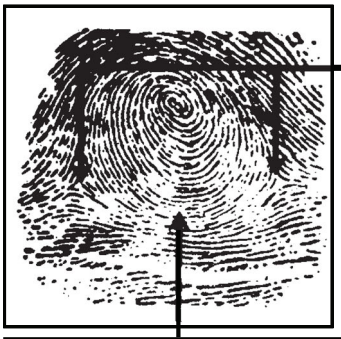
APPLICANT

1. LOOP



THE LINES BETWEEN CENTER OF LOOP AND DELTA MUST SHOW

2. WHORL



THESE LINES RUNNING BETWEEN DELTAS MUST BE CLEAR

3. ARCH



ARCHES HAVE NO DELTAS

FD-258 (REV. 5-15-17)

THIS CARD FOR USE BY:

1. LAW ENFORCEMENT AGENCIES IN FINGERPRINTING APPLICANTS FOR LAW ENFORCEMENT POSITIONS.*
2. OFFICIALS OF STATE AND LOCAL GOVERNMENTS FOR PURPOSES OF EMPLOYMENT, LICENSING, AND PERMITS, AS AUTHORIZED BY STATE STATUTES AND APPROVED BY THE ATTORNEY GENERAL OF THE UNITED STATES. LOCAL AND COUNTY ORDINANCES, UNLESS SPECIFICALLY BASED ON APPLICABLE STATE STATUTES DO NOT SATISFY THIS REQUIREMENT.*
3. U.S. GOVERNMENT AGENCIES AND OTHER ENTITIES REQUIRED BY FEDERAL LAW.**
4. OFFICIALS OF FEDERALLY CHARTERED OR INSURED BANKING INSTITUTIONS TO PROMOTE OR MAINTAIN THE SECURITY OF THOSE INSTITUTIONS.

Please review this helpful information to aid in the successful processing of hard copy civil fingerprint submissions in order to prevent delays or rejections. Hard copy fingerprint submissions must meet specific criteria for processing by the Federal Bureau of Investigation.

Ensure all information is typed or legibly printed using blue or black ink.
Enter data within the boundaries of the designated field or block.
Complete all required fields. (If a required field is left blank, the fingerprint card may be immediately rejected without further processing.)

- The required fields for hard copy civil fingerprint cards are: ORI, Date of Birth, Place of Birth, NAM, Sex, Date fingerprinted, Reason Fingerprinted, and proper completion of fingerprint impression boxes.

Do not use highlighters on fingerprint cards.
Do not enter data or labels within 'Leave Blank' areas.
Ensure fingerprint impressions are rolled completely from nail to nail.
Ensure fingerprint impressions are in the correct sequence.
Ensure notations are made for any missing fingerprint impression (i.e. amputation).
Do not use more than two retabs per fingerprint impression block.
Ensure no stray marks are within the fingerprint impression blocks.

Training aids can be ordered online via the Internet by accessing the FBI's website at: fbi.gov, click on 'Fingerprints', then click on 'Ordering Fingerprint Cards & Training Aids'. Direct questions to the Biometric Services Section's Customer Service Group at (304) 625-5590 or by e-mail at <identity@fbi.gov>.

Social Security Account Number (SSAN): Pursuant to the Privacy Act of 1974, any Federal, state, or local government agency that requests an individual to disclose his or her SSAN, is responsible for informing the person whether disclosure is mandatory or voluntary, by what statutory or other authority the SSAN is solicited, and what uses will be made of it. In this instance, the SSAN is solicited pursuant to 28 U.S.C 534 and will be used as a unique identifier to confirm your identity because many people have the same name and date of birth. Disclosure of your SSAN is voluntary; however, failure to disclose your SSAN may affect completion or approval of your application.

PRIVACY ACT STATEMENT

Authority: The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Pub.L. 92-544, Presidential Executive Orders, and federal regulations. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.

Principal Purpose: Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems (including civil, criminal, and latent fingerprints repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.

Routine Uses: During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting, licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

PAPERWORK REDUCTION ACT NOTICE

According to the Paperwork Reduction Act of 1995, no persons are required to provide the information requested unless a valid OMB control number is displayed. The valid OMB control number for this information collected is 1110-0046. The time required to complete this information collected is estimated to be 10 minutes, including time reviewing instructions, gathering, completing, reviewing and submitting the information collection. If you have any comments concerning the accuracy of this time estimate or suggestions for reducing this burden, please send to: Department Clearance Officer, United States Department of Justice, Justice Management Division, Policy and Planning Staff, Washington, DC 20530.

INSTRUCTIONS:

* 1. PRINTS MUST GENERALLY BE CHECKED THROUGH THE APPROPRIATE STATE IDENTIFICATION BUREAU, AND ONLY THOSE FINGERPRINTS FOR WHICH NO DISQUALIFYING RECORD HAS BEEN FOUND LOCALLY SHOULD BE SUBMITTED FOR FBI SEARCH.

2. IDENTITY OF PRIVATE CONTRACTORS SHOULD BE SHOWN IN SPACE "EMPLOYER AND ADDRESS". THE CONTRIBUTOR IS THE NAME OF THE AGENCY SUBMITTING THE FINGERPRINT CARD TO THE FBI. UNIVERSAL CONTROL NUMBER, IF KNOWN, SHOULD ALWAYS BE FURNISHED IN THE APPROPRIATE SPACE.

** 3. MISCELLANEOUS NO. - RECORD: OTHER ARMED FORCES NO. PASSPORT NO. [FP], ALIEN REGISTRATION NO. (AR), PORT SECURITY CARD NO. (PS), SELECTIVE SERVICE NO. (SS) VETERANS' ADMINISTRATION CLAIM NO. (VA).

EXHIBIT J

CONTRACTOR PERSONNEL ROLLOVER REQUEST FORM

Social Security Administration (SSA) *Center for Suitability and Personnel Security (CSPS)*

Submit this document to your designated contracting officer's representative-contracting officer's technical representative (COR-COTR) via secure email. The COR-COTR must ensure the information is complete and accurate (all fields are required) and then submit to ^DCHR OPE Suitability.

Only use this form when contractor personnel already working on an SSA contract need to move to another SSA contract. The information on this form must be typed, complete, and accurate. Failure to do so may result in a delay in receiving a suitability letter. The company point of contact (CPOC) and COR-COTR will receive suitability letters from the Center for Suitability and Personnel Security (CSPS) once the rollover is complete.

FULL NAME	SOCIAL SECURITY NUMBER	DATE OF BIRTH	FROM	TO	ACTIVE ON BOTH CONTRACTS?	
LAST FIRST MIDDLE	*000-00-0000*	*MM/DD/YYYY*	*CONTRACT NUMBER*	*CONTRACT NUMBER*	*YES*	*NO*
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐

CPOC INFORMATION:

NAME: _____ EMAIL ADDRESS: _____

PHONE: _____ DATE OF SUBMISSION:_____

COR-COTR INFORMATION:

NAME: _____ EMAIL ADDRESS: _____

PHONE: _____

EXHIBIT K

Security and Privacy Awareness Training
Contractor / Affiliate Personnel Security Certification

Purpose:

This training document is to be signed by contractor, subcontractor, or affiliate personnel, and those acting on behalf of the Social Security Administration (SSA) who have been granted access to SSA information and information systems to certify that they have received and understand SSA Information Security and Privacy Awareness Training detailed below.

Background:

SSA is vital to the economic security of the United States. In the performance of their duties in support of SSA's mission, all contractors, subcontractors, affiliates, and those acting on behalf of SSA who have been granted access to SSA information systems, hereafter referred to as "Authorized Users(s)," are responsible for protecting such information and information systems (e.g., hardware, software/applications, federal information/data, network, people) throughout the entire information life cycle, including collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Federal information includes information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Security awareness training is required for Authorized Users, per Section 44 USC 3554 of the Federal Information Security Modernization Act of 2014 (FISMA). Failure to follow prescribed rules or misuse of federal information and information systems can lead to criminal penalties, including fines and imprisonment, and disciplinary actions according to the contract and/or agreement under which I am performing work for SSA.

I understand that SSA maintains a variety of sensitive information about the agency's operations and programs, which may be information pertaining to program (e.g., information about SSA's clients) or non-program (e.g., administrative and personnel records) matters. I understand that SSA may authorize me to have access to federal information and information systems and that my access to and use of such information and information systems must be in accordance with the provisions of the contract and/or agreement under which I am performing work for SSA.

I understand that the terms in the contract and/or agreement under which I am performing work for SSA take precedence over this document. I understand that any questions I may have concerning authorization(s) to access SSA information and information systems should be directed in accordance with the terms of the contract and/or agreement. I have read, understand, and agree to the following conditions:

Insider Threat

An insider threat is someone with authorized access who uses that access, intentionally or unintentionally, to harm the security of the Agency or the Nation. The individual with authorized access may attempt to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities.

- If I observe a potential insider threat, **I will** report the incident to SSAITP@ssa.gov and, as appropriate, in accordance with the personally identifiable information and incident reporting requirements in the contract or agreement under which I am working.
- **I will** safeguard federal information and information systems from exploitation, compromise, espionage, terrorism, or other unauthorized use and disclosure.

Malware, Remote Access, and Mobile Device Security

Malware encompasses malicious software, programs, files, and/or code in the form of virus, ransomware, and spyware that cause damage to information systems and data. SSA defends against malware using antivirus programs, intrusion detection systems, and social engineering training among other methods. Routine software and security updates ensure SSA devices are up to date with the latest malware protection.

When I have been granted an SSA device to perform work for the agency, the following requirements apply:

- In order to ensure my SSA device receives the necessary software and security updates**, I will** remain connected to SSANet using the agency's Virtual Private Network throughout my workday**, I will** keep my workstation plugged in and powered on, and **I will** restart my workstation at least once a week and at the end of each workday, logging off from the CTRL+ALT+DELETE screen unless further guidance is issued.

- **I will not** store federal information on personally owned media devices or, connect non-SSA approved and issued personal Bluetooth devices to an SSA device.

- **I will not** alter SSA devices, disable security settings, or download or install unauthorized software onto SSA devices.

- **I will** follow the security and safety requirements of any alternative worksite agreement and all contract or agreements related to non-SSA worksites.

- **I will not** print any material that contains federal information at an unapproved location. **I will** protect SSA devices at all times, to include while on travel, at any alternative worksite, and any approved non-SSA worksite.

Secure Browsing and Social Media

Attackers use social data mining techniques to gather information about an individual or organization in public or social settings, including social media. SSA social media accounts are not official SSA websites, but rather the department's presence on third-party service providers' platforms, which means SSA has limited control over how each platform uses personal data provided by users.

- **I will not** transmit, store, or process federal information on non-SSA owned and operated sites, including social media, third party online forums, third-party collaboration tools or sites, social networking sites, any other non-SSA-hosted sites, or unapproved third-party data storage providers unless explicitly authorized to do so.

- **I will not** share programming code used for federal information systems with unauthorized individuals including but not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

- **I will not** use federal information systems to browse or access information about myself, my children, other family members, co-workers or former co-workers, acquaintances, and/or friends.

Secure Email and Fax Use

Email is an official business communication tool and users must use it in a responsible, secure, and lawful manner. When using SSA email, to protect agency systems and those who receive email from me:

- **I will** use business communication tools including SSA email in a responsible, secure, and lawful manner.
- **I will not** send or forward Personally Identifiable Information (PII) to or from a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List.
- **I will not** copy or blind copy work-related email to a personal, non-SSA email address.
- **I will not** send or forward chain letters or other unauthorized mass mailings.
- **I will not** configure my SSA email account to automatically forward work-related email to an outside (non-SSA, non-secure) address.
- If I receive an email intended for someone else, **I will** immediately notify the sender and delete or destroy the misdirected message.

A fax is an official business communication tool and users must use it in a responsible, secure, and lawful manner. When using an SSA fax, to protect agency systems and those who receive faxes from me:

- **I will** use business communication tools including SSA fax in a responsible, secure, and lawful manner.
- **I will** use a cover sheet that notes the sensitivity of the material and follow all Controlled Unclassified Information (CUI) labeling requirements.
- **I will not** leave fax machines unattended when transmitting.
- **I will** transmit faxes to the intended recipient, when possible, using pre-programmed fax numbers.
- **I will not** use SSA's fax system to create or distribute disruptive or offensive messages.
- If I receive a fax by mistake, **I will** notify the sender. To the extent possible, **I will not** read the fax's contents. **I will** destroy the misdirected message.

Security Incident Reporting

Security incidents involve any attempted or actual authorized access, use, disclosure, modification, or destruction of information. Examples include malicious or unauthorized intrusion or access, virus attacks, phishing, vishing, supply chain threats, foreign intelligence threats, insider threats, and loss of PII.

- If I suspect or confirm the loss or theft of any sensitive information, including PII, **I will** report it within one hour to my supervisor, manager, contracting officer's representative and/or contracting officer's technical representative or another designated official. If those individuals are not available, **I will** use the PII Loss Reporting Tool to report any loss or theft of any sensitive information or PII.
- If I observe a suspected systems intrusion attempt or other security-related incident, **I will** report the incident within 15 minutes of discovery to SOC@ssa.gov.
- If I am the targeted victim of a phishing (suspicious email) attempt, **I will** report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- If I am the target of a vishing (suspicious phone call) attempt, **I will** report the incident within 15 minutes of discovery to SOC@ssa.gov.
- If I observe a potential insider threat, **I will** report the incident to SSAITP@ssa.gov. If I observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, **I will** report the incident to the Office of the Inspector General in accordance with published policy.

Social Engineering

Vishing is the practice of tricking you, over the phone, into revealing information to an unauthorized individual or performing actions on your workstation that may compromise the security of SSA.

- **I will** avoid vishing attempts by validating a caller's identity and purpose.
- If I am unable to validate the caller's identity, **I will** hang up and call back using a number I know to be correct.

Phishing is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.

- **I will** avoid phishing attempts by verifying the email sender.
- **I will** be suspicious when receiving emails from individuals I do not know or have not heard from in a long time.
- **I will** never respond to requests for PII or send password information in an email.
- **I will** only release information if I am confident of an individual's identity and right to receive it.

Unauthorized Access and Prohibited Behavior

Unauthorized access to federal information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Federal information system users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time, including accessing the Internet using E-mail.

- **I will not** inspect, access, or attempt to access any federal information that SSA has not expressly authorized me to access.
- **I will not** release or disclose any federal information to any unauthorized person, agency, or entity. **I understand** that unauthorized disclosure of federal information may lead to civil penalties and/or criminal prosecution under Federal law (e.g., The Privacy Act of 1974, 5 U.S.C. 552a; SSA's regulations at 20 C.F.R. Part 401; The Social Security Act, 42 U.S.C. 1306 (a); and 5 U.S.C. Section 552(i)). **I further understand** that additional privacy and disclosure protections may apply to certain types of SSA information including Federal Tax Information (i.e., earnings information), which may be subject to additional penalties under sections 6103, 7213, 7213A, and 7431 of the Internal Revenue Service (IRS) Code (Title 26 of the United States Code).
- **I will** follow all access, retention, and/or destruction requirements in the contract and/or agreement under which I am authorized to access federal information. **I understand** that such requirements may require me to cease access to, return, or destroy federal information upon completion of my work for SSA or termination of my contract and/or agreement that authorized my access to federal information.
- **I will not** take federal information off-site, unless expressly authorized to do so by contract and/or agreement or other written authorization from SSA. If SSA authorizes me to take federal information off-site, I agree to safeguard all such information in accordance with agency policy and standards and the requirements of the contract and/or agreement under which I am performing work so that no unauthorized person, agency, or entity can access federal information.
- **I will** keep confidential any third-party proprietary information that may be entrusted to me as part of the contract and/or agreement, including safeguarding such information from unauthorized access and not disclosing or releasing such information unless expressly authorized to do so.
- **I will** follow all requirements in the contract and/or agreement under which I am performing work for SSA, includingbut not limited to those governing confidential information or PII.
- **I will** only use my access to federal information and information systems for the performance of my official duties.

Contractor Employee Name (Print/Type)	Date (MM/DD/YYYY)
Contractor Employee Signature (Sign)	

Contract Number	Company Name (Print/Type)
Company Point Of Contact (Print/Type)	Company Point of Contact Phone Number

Privacy Act
Collection and Use of Personal Information

42 U.S.C. § 904(a); 20 C.F.R. § 401.90; 44 U.S.C. §§ 3541-3549; 41 C.F.R. Chapter 101; 5 U.S.C. § 552a(e)(9)-(10); and Executive Order 13488 of the Social Security Act, as amended, allow us to collect this information. Furnishing this information to the Social Security Administration (SSA) is voluntary. However, failing to provide this information may affect your ability to access Federal information and information systems, which is a condition of the contract under which you are performing work for SSA (SSA contract). Not providing this information also could prevent us from issuing you a PIV credential and/or authorizing you to access SSA's network, one or both of which may be conditions of your SSA contract. Failure to follow prescribed rules or misuse of SSA information and information systems could lead to removal from duty from your SSA contract.

We will use the information you provide to grant you access to Federal information and information systems. We may also share your information for the following purposes, called routine uses:

- To contractors and other Federal agencies, as necessary, for assisting SSA in the efficient administration of its programs. We disclose information under this routine use only in situations in which SSA may enter into a contractual or similar agreement with a third party to assist the accomplishing an agency function relating to this system of records; and

- To student volunteers, individuals working under a personal services contract, and other workers who individuals performing functions for SSA but technically do not having the status of Federal agency employees, when they are performing work for SSA, as authorized by law, and if they need access to personally identifiable information (PII) in SSA the records in order to perform their assigned agency functions.

In addition, we may share this information in accordance with the Privacy Act and other Federal laws. For example, where authorized, we may use and disclose this information in computer matching programs, in which our records are compared with other records to establish or verify a person's eligibility for Federal benefit programs and for repayment of incorrect or delinquent debts under these programs.

A list of additional routine uses is available in our Privacy Act System of Records Notice (SORN) 60-0361, entitled Identity Management System, as published in the Federal Register (FR) on November 3, 2006, at 71 FR 64751. Additional information, and a full listing of all our SORNs, is available on our website at www.ssa.gov/privacy.

EXHIBIT L

Social Security Administration

Cybersecurity Supply Chain Risk Assessment (CSCRA) Questionnaire

All questions on this questionnaire must be answered completely and accurately to be considered for award on a contract for the production of products required by the Social Security Administration (SSA). Incomplete or inaccurate forms may not be considered. (See "SSA Provision" at the end of this questionnaire for more information.)

NOTE: All references to "contractor" throughout this document refer to the contractor in line for award. The contractor in line for award is required to provide the information below as applicable to the contract being considered for award.

CONTRACTOR COMPANY INFORMATION

1. The contractor must provide the following information on their company:

Company Name	
Main Address	
DUNS # **UEI#**	
State of Incorporation	
Website	
Org. Type (LLC, Partnership, etc.)	
Trade Names, DBA	
Foreign Affiliations/ Ownership (Locations, significant individual/entity shareholders, subsidiaries)	

CONTRACTOR EXECUTIVE INFORMATION

2. The contractor must provide the following information for the Executives affiliated with the above-specified company. This information must include the chief executive officer or president, owner(s), vice presidents, and chief financial officers.[1] If there is a web link to the company's leadership, that information must be provided as well.

Name (First, Middle, Last)	Title	Resident City, State	Year of Birth	Citizenship	% Ownership of Awardee Company

[1] Note: This information is necessary in order to confirm/rule out results derived during the due diligence process.

SUBCONTRACTOR COMPANIES (AS APPLICABLE):

3. For all subcontractors involved in the supply chain of the product(s) or service(s) being provided to SSA or needed by the contractor in the production of SSA products, the contractor must provide the information below. This information includes, but is not limited to, resellers, suppliers, distributors, and manufacturers, as applicable to the contract (see "NOTE" below). The address information should include from where the software or hardware being provided/used is supplied, distributed, or manufactured, if applicable. *Use and attach additional, separate sheet(s), as needed.*

NOTE: For the purpose of this questionnaire, the information below regarding subcontractors is in reference to any IT operations, hardware, or software being provided to SSA or used in the production of SSA products, including but not limited to, production, processing, storage, transfer, and disposal of SSA data.

	Subcontractor 1	**Subcontractor 2**	**Subcontractor 3**
Type (reseller, supplier, manufacturer, etc.)			
Company Name			
DUNS# UEI#			
Headquarters/ Mailing Address			
Product-specific Facility Address(es)[2] (name, address, type, purpose)			
Foreign Affiliations/ Ownership (locations, ownership, significant individual/entity shareholders and percentages)			

SUBCONTRACTOR EXECUTIVE INFORMATION (IF APPLICABLE)

4. The contractor must provide the following information for the executives affiliated with the above-specified subcontractor companies (see "NOTE" under 3. "Subcontractor Companies"). This information must include the chief executive officer or president, owner(s), any vice presidents, and any chief financial officers.[3]

[2] For each facility where any information system, IT hardware or software will be designed, manufactured, packaged, and stored prior to distribution, as applicable.
[3] Note: This information is necessary in order to confirm/rule out results derived during the due diligence process.

If there is a web link to the company's leadership, that information must be provided as well.

Name (First, Middle, Last)	Company	Title	Resident City, State	Year of Birth	Citizenship

HARDWARE AND SOFTWARE (AS APPLICABLE TO THE CONTRACT):

5. For all entities identified in Questions 1. "Contractor Company" and 3. "Subcontractor Companies," the contractor must provide the name, purpose, and product number of the hardware or software being provided/used by each entity listed, if applicable. *Use and attach additional, separate sheet(s), as needed.*

Hardware Information

	Contractor Company	Subcontractor 1	Subcontractor 2	Subcontractor 3
Company Name				
Product Name				
Product Number				
Purpose				

Software Information

	Contractor Company	Subcontractor 1	Subcontractor 2	Subcontractor 3
Company Name				
Product Name				
Product Number				
Purpose				

SHIPPING AND DELIVERY

6. If applicable to the contract, in the table below, contractor must provide details on how the IT hardware/software products will be shipped and/or delivered to SSA. Add additional rows, if needed. If not applicable, insert "Not Applicable" or "N/A."

Hardware Information

Product Name	Delivery Method	Storage Method	Transportation Company

Software Information

Product Name	Delivery Method	Storage Method	Software Delivery Provider

SECURITY PROGRAMS

7. For all entities identified in Questions 1. "Contractor Company" and 3. "Subcontractor Companies," (if applicable - see "NOTE" under 3. "Subcontractor Companies"), the contractor must provide evidence that they maintain the programs/systems listed below. This answer must provide evidence of each, which can be direct company policy wording. Contractor must provide any evidence if the contractor or subcontractor(s) is International Organization for Standardization (ISO) certified. *Use and attach additional, separate sheet(s), as needed.*

Name	Personnel Security	Cybersecurity	Physical Security	Supply Chain	ISO Certified ?
Contractor Company					
Subcontractor 1					
Subcontractor 2					
Subcontractor 3					

SERVICE/MAINTENANCE AGREEMENTS (IF APPLICABLE)

8. Does the proposed information system, IT hardware or software include a service/maintenance agreement?

____ Yes

____ No

9. If yes, contractor must provide the following information of the contractor/subcontractor(s) who will provide the service:

Service Company Name	
Company Address	
DUNS# **UEI#**	
Delivery Method (i.e. on-site, remote via internet)	
Location where Service is provided from	
Citizenship of employees providing service/maintenance	

STORAGE AND SANITATION/DISPOSAL SERVICES (IF APPLICABLE)

10. What entity/entities will provide the storage and sanitation/disposal services of any proposed information system and IT hardware or software? If so, how? If it is a virtual service, insert "N/A."

11. Record of sanitation/disposal - how will the entity assure no traceability and no recovery?

BILL OF MATERIAL LISTS (IF APPLICABLE)

12. Are the Bill of Material lists maintained for all hardware and software delivered under the contract? If so, where can they be accessed? If not applicable to the contract, insert "N/A."

CYBERSECURITY/DATA BREACHES

13. For all entities identified in Questions 1. "Contractor Company" and 3. "Subcontractor Companies," have any of the companies listed experienced a security/data breach in the last 24 months? If yes, contractor must provide the details concerning the breach. (Refer to all applicable National Institute of Standards and Technology (NIST) publications and Executive Orders in reference to data security.)

SSA PROVISION

To the maximum extent practicable, the contractor shall submit all required CSCRA information in a single, unified report. Therefore, it is incumbent on the contractor to coordinate with its subcontractors (including suppliers, distributors, manufacturers, and any other entities involved in the contractor's supply chain – see "NOTE" under 3. "Subcontractor Companies" for more information) to collect and compile all required CSCRA information as applicable to the contract.

Upon submission of the CSCRA information, the contractor is attesting to the truthfulness of that information.

The Government will not sign non-disclosure agreements from the contractor or any of their subcontractors.

All required CSCRA information submitted in response to this solicitation will be handled in accordance with the policies and procedures of the Government Publishing Office (GPO) and Social Security Administration.

The contractor must submit a completed CSCRA questionnaire in accordance with the contract specifications.

Failure to provide all required CSCRA information, as applicable to the contract being considered for award, may result in the contractor being declared non-responsible.

EXHIBIT M

SYSTEM PLAN

TYPE OF PROPOSED MAINFRAME PLATFORM_____

TYPE OF PERSONAL COMPUTER_____

MEDIA TO BE USED FOR RECEIPT OF FILE TRANSMISSION_____

FILE STORAGE MEDIUM_____

MANAGED FILE TRANSFER PLATFORM SERVER INSTALLED?_____

AMOUNT OF AVAILABLE FILE STORAGE SPACE_____

TYPE OF PRINT STREAM MAIL RUN CONTROL SYSTEM_____

TYPE OF NETWORK PLATFORM (i.e., NOVELL/NT/UNIX)_____

EXHIBIT N

100% Accountability and Summary Reports

Full Audit report must include the following information (reprints must have the same information):

1. Program Number/Job Name/Print Order/File Date
2. PC#/Sequence numbers/Total Volume
3. Inserter ID and Operator
4. Date of insertion
5. Start and End time
6. Start and End Range (sequence numbers)
7. Total for each Start and End Range
8. Event (i.e. Processed, Spoiled, Diverted and reason: Missing Piece, Unverified, Misread etc.)
9. Status (i.e. Inserted, Routed to Reprint Area, etc.)
10. Totals
    a. Machine inserted
    b. Sent to Reprint
    c. Reprints Recovered
    d. Records Accounted For
    e. Duplicates
    f. Duplicated Verified
    g. Records less duplicates
    h. Reported Output
    i. Variances

Example:

Audit Report

Program 123-S/SSA Notices Name/PO#54001/File Date

PC # and Sequence Numbers and Volume

Inserter ID	Date	Start Time	End Time	Start Range	End Range	Total	EVENT	STATUS
Inserter 1	05/10/12	10:31:04 AM	11:12:45 AM	19386	21567	2182	Standard Processing	Inserted
Operator Joe	05/10/12	11:12:50 AM	11:12:50 AM	21568		1	Diverted	Routed to Reprint
	05/10/12	11:13:10 AM	11:28:06 AM	21569	22516	948	Standard Processing	Inserted
	05/10/12	11:28:07 AM	11:28:10 AM	22517	22518	2	Diverted/ leave count unverified	Routed to Reprint
	05/10/12	11:29:30 AM	11:29:35 AM	22519	22521	3	Diverted/missing piece	Routed to Reprint
	05/10/12	11:29:45 AM	11:30:15 AM	22522		1	Diverted/manual insertion of pub	Manual Scan
	05/10/12	11:30:34 AM	11:40:35 AM	22523		1	Diverted/misread	Manual Scan
Inserter 2	05/11/12	8:12:50 AM	8:12:50 AM	21568		1	Standard Processing	Inserted
(REPRINTS)	05/11/12	8:28:07 AM	8:28:10 AM	22517	22518	2	Standard Processing	Inserted
Operator Sue	05/11/12	8:29:30 AM	8:29:35 AM	22519	22521	3	Standard Processing	Inserted

TOTALS	
Machine Inserted:	26604
Sent to Reprints:	582
Reprints Recovered:	582
Records Accounted for:	27186
Duplicates:	16
Duplicates Verified:	16
Records Less Duplicates:	27170
Reported Output:	27170
Variance:	0

The Summary Report must include the following; Reprints must also have all of the same information:

1. Job Name/Print Order
2. Piece Quantity
3. Sequence number range (Start and End Range)
4. Start date and time
5. End date and time
6. Total Processed Pieces
7. Total Reprints
8. Total Pieces Inserted
9. Total Variances
10. Job Complete or Incomplete

Summary Report

Job Information

Job Name:	XYZ Notice	
PO #	54001	
Piece Quantity:	35862	
Job Status:	Completed	
Start Date &Time:	05/10/12	10:29:54
End Date & Time:	05/11/12	14:22:34

Operation Information

Start Range:	1
End Range	35862

Statistical Summary

35537 Processed Pieces -	Completed 05/10/12 10:29:54
325 Processed Reprints -	Completed 05/11/12 14:22:34
35862 Total Pieces Inserted -	Completed 05/11/12 14:22:34
0 Variances -	Job Complete