Program:	096-S											
Term:	September 1, 2021 to August 31, 2022											
Title:	EAD, YCER, BEVE, and eRPA Notices											
			SOURCELINK OHIO dba									
			AMSIVE OH.		**IMS, INC.**		**NPC, INC.**		**PINNACLE DATA SYSTEMS**		**CURRENT CONTRACTOR**	
		BASIS OF	MIAMISBURG, OH		LIVERPOOL, NY		CLAYSBURG, PA		SUWANEE, GA		PINNACLE DATA SYSTEMS	
ITEM NO.	DESCRIPTION	AWARD	UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**
I.	**COMPOSITION:**											
(a)	Envelopes……per envelope……..	8	$10.00	$80.00	No Charge	$0.00	$50.00	$400.00	No Charge	$0.00	No Charge	$0.00
II.	**PROCESSING /FORMATTING FILES:**											
(a)	Processing/Formatting Files……..per Mailer……..	9	No Charge	$0.00	No Charge	$0.00	$50.00	$450.00	No Charge	$0.00	No Charge	$0.00
III.	**PREPRODUCTION TESTS:**											
(a)	Transmission Test……per test……..	1	No Charge	$0.00	No Charge	$0.00	No Charge	$0.00	No Charge	$0.00	No Charge	$0.00
(b)	Preproduction Validation Tests……..per test……..	1	No Charge	$0.00	No Charge	$0.00	No Charge	$0.00	No Charge	$0.00	No Charge	$0.00
(c)	Payment Stub Validation Test (eRPA OP1 only)……per test……..	1	No Charge	$0.00	No Charge	$0.00	No Charge	$0.00	No Charge	$0.00	No Charge	$0.00
IV.	**PRINTING, IMAGING, BINDING AND CONSTRUCTION:**											
(a)	* Daily Makeready/Setup Charge	250	$200.00	$50,000.00	$110.00	$27,500.00	$174.24	$43,560.00	No Charge	$0.00	No Charge	$0.00
(b)	Notice Leaves……per 1,000 leaves…	15,076	$11.75	$177,143.00	$11.00	$165,836.00	$7.40	$111,562.40	$11.25	$169,605.00	$12.00	$180,912.00
(c)	White CRM Envelope (5-3/4 x 8-3/4")……per 1,000 envelopes…	23	$14.60	$335.80	$10.40	$239.20	$14.86	$341.78	No Charge	$0.00	No Charge	$0.00
(d)	White BRM Envelope (5-3/4 x 8-3/4")……per 1,000 envelopes…	149	$9.85	$1,467.65	$10.40	$1,549.60	$14.86	$2,214.14	No Charge	$0.00	No Charge	$0.00
(e)	Green BRM Envelope (3-7/8 x 8-7/8')……per 1,000 envelopes…	50	$17.78	$889.00	$33.80	$1,690.00	$32.04	$1,602.00	No Charge	$0.00	No Charge	$0.00
(f)	Mail-Out Envelope (4-1/8 x 9-1/2")…… per 1,000 envelopes…	5,352	$7.97	$42,655.44	$11.00	$58,872.00	$8.44	$45,170.88	No Charge	$0.00	No Charge	$0.00
(g)	Mail-Out Envelope (6-1/8 x 9-1/2")……per 1,000 envelopes…	2,186	$11.67	$25,510.62	$12.98	$28,374.28	$11.20	$24,483.20	No Charge	$0.00	No Charge	$0.00
V.	**PAPER: Per 1,000 leaves**											
(a)	Personalized Notices: White OCR Bond (20-lb.)	15,056	$8.56	$128,879.36	$7.96	$119,845.76	$5.02	$75,581.12	$6.50	$97,864.00	$6.50	$97,864.00
(b)	White CRM Envelope (5-3/4 x 8-3/4"): White Writing envelope (20-lb.)	23	$14.60	$335.80	$6.80	$156.40	$14.86	$341.78	$12.50	$287.50	$14.50	$333.50
(c)	White BRM Envelope (5-3/4 x 8-3/4"): White Writing envelope (20-lb.)	149	$9.85	$1,467.65	$6.80	$1,013.20	$14.86	$2,214.14	$12.50	$1,862.50	$22.00	$3,278.00
(d)	Green BRM Envelope (3-7/8 x 8-7/8"): Green Writing envelope (20-lb.)	50	$17.78	$889.00	$22.55	$1,127.50	$32.04	$1,602.00	$19.00	$950.00	$12.50	$625.00
(e)	Mail-Out Envelope (4-1/8 x 9-1/2): White Writing envelope (24-lb.); or at contractor's option, White Uncoated Text (60-lb.)	5,352	$7.97	$42,655.44	$6.65	$35,590.80	$8.44	$45,170.88	$14.50	$77,604.00	$12.50	$66,900.00
(f)	Mail-Out Envelope (6-1/8 x 9-1/2"): White Writing envelope (24-lb.); or at contractor's option, White Uncoated Text (60-lb.)	2,186	$11.67	$25,510.62	$8.60	$18,799.60	$11.20	$24,483.20	$20.00	$43,720.00	$19.00	$41,534.00
VI.	**INSERTING AND MAILING:**											
(a)	Mailers……per 1,000 Mailers…	7,538	$20.00	$150,760.00	$8.79	$66,259.02	$12.20	$91,963.60	$10.00	$75,380.00	$10.00	$75,380.00
	CONTRACTOR TOTALS			**$648,579.38**		**$526,853.36**		**$471,141.12**		**$467,273.00**		**$466,826.50**
	DISCOUNT		**0.00%**	$0.00	**0.00%**	$0.00	**0.25%**	$1,177.85	**1.00%**	$4,672.73	**1.00%**	$4,668.27
	DISCOUNTED TOTALS			**$648,579.38**		**$526,853.36**		**$469,963.27**		**$462,600.27**		**$462,158.23**
				AWARDED								

U.S. GOVERNMENT PUBLISHING OFFICE
Washington, DC

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

EAD, YCER, BEVE, and eRPA 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 from **September 1, 2021** and ending **August 31, 2022**, plus up to four (4) optional 12-month extension period(s) that may be added in accordance with the "OPTION TO EXTEND THE TERM OF THE CONTRACT" clause in SECTION 1 of this contract.

Contractor interfacing with SSA's National File Transfer Management System (FTMS) for electronic transmission of files from SSA to the production facility will take place from September 1, 2021 through November 30, 2021. Transmission of live production files will commence on December 1, 2021.

BID OPENING: Bids shall be opened at 11:00 a.m., prevailing Washington, DC Time, on **June 14, 2021**, at the Government Publishing Office, Washington, DC. (Due to the COVID-19 pandemic, this will NOT be a public bid opening.)

BID SUBMISSION: Due to the COVID-19 pandemic, the physical office will NOT be open. Based on this, bidders must submit email bids to bidsapsdc@gpo.gov for this solicitation. No other method of bid submission will be accepted at this time.

The program 096-S and bid opening date must be specified in the subject line of the emailed bid submission. Bids received after 11:00 a.m. on the bid opening date specified above will not be considered for award.

BID RESTRICTION: Due to travel restrictions as a result of COVID-19, bidders must have an SSA pre-approved security clearance at the bidder's physical location(s) that will be used in the production of products for this contract.

NOTE: If bidder does not have these requirements completed *prior* to bid submission, the bidder will be declared non-responsible.

BIDDERS, PLEASE NOTE: These specifications have been revised; therefore, all bidders are cautioned to familiarize themselves with all provisions of these specifications before bidding, with particular attention to "SECURITY AND SUITABILITY REQUIREMENTS FOR GOVERNMENT PRINTING (NOV 2018)" and "100% ACCOUNTABILITY OF PRODUCTION AND MAILING" requirements.

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, call **David Love** at (202) 512-0307 or email dlove@gpo.gov

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 laser/ion deposition imaging, inserting of data from electronically transmitted files, and disposal/destruction of waste materials. Any bidder who cannot perform the predominant production functions of this contract will be declared non-responsible. (**NOTE**: Inkjet printing is not allowed.)

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

If the presorting and mailing is subcontracted, the subcontractor must complete and pass the same security clearances as the prime contractor.

If the contractor wishes 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 a new subcontractor's information to the Government for approval 30 calendar days prior to the start of production at that facility.

If the contractor plans to enter into a "Contractor Team Arrangement" or Joint Venture to fulfill any requirements of this contract, they must comply with the terms and regulations as detailed in the Printing Procurement Regulation (GPO Publication 305.3; Rev. 4-14).

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

Product Quality Levels:

(a) Printing (page related) Attributes – Level III.
(b) Finishing (item related) Attributes – Level III.

Inspection Levels (from ANSI/ASQC 1.4):

(a) Non-destructive Tests - General Inspection Level I.
(b) Destructive Tests - Special Inspection Level S-2.
(c) Low-gloss, transparent, 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 USPS OCR Scanner.
(d) Exception: ANSI X3.17 "Character Set for Optical Character Recognition (OCR A)" must apply to these specifications. The revisions of this standard which are effective as of the date of this contract are those which must apply.
(e) Exception: The notices (front and back) will be read by a high-speed document scanner. These notices must function properly when processed through a high-speed document scanner. A form is a reject and will be considered a major defect when its OCR print cannot be correctly deciphered on the first pass through the specified reading equipment.

(f) Exception: Data Matrix 2-D barcodes must be in accordance with ISO/IEC 16022 – "International Symbology Specification, Data Matrix;" ISO/IEC 15418:1999 – "Symbol Data Format Semantics;" ISO/IEC 15434:1999 – "Symbol Data Format Syntax;" and ISO/IEC 15415 – "Print Quality Standard."

(g) Exception: Code 39 (3 of 9) barcodes must be in accordance with ANSI MH 10.8M-1983.

(h) Exception: The payment portion below the micro-perforation on the "payment stub" (eRPA SSA-L732-OP1), once detached, will be scanned and must function properly when processed through the current high-speed scanning equipment at SSA. The payment stub produced requires precision spacing, printing, and trimming. It is critical that the bottom of the OCR-A scanline be 1/2" from the bottom of the payment stub page and that, when reading from the right, the first encodable character is encountered at least 1/4" but no more than 5/16" (plus or minus 1/16") from the right leading edge of the payment stub. A form is a reject and will be considered a major defect when its OCR print cannot be correctly deciphered on the first pass through the scanning equipment (See "PRINTING/IMAGING" for eRPA SSA-L732-OP1and "BINDING" for additional information regarding perforated payment stub.)

NOTE: Use of equipment or ink which in any way adversely affects the scannability of the payment stub will not be allowed. 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 must be:

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

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

P-7. O.K. Preproduction Test Samples; O.K. Proofs; Electronic Media; Camera/Manuscript Copy.

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 **September 1, 2021** to **August 31, 2022**, 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 **May 31, 2021** 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 production begins December 1, 2021.

1. BLS code 0913 for <u>All Paper</u> will apply to all paper required under this contract.

2. The applicable index figures for the month of **November 2021** 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 is 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 V., "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.

ALL REQUIREMENTS, STARTING WITH "SECURITY REQUIREMENTS" BELOW, THROUGH THE SECTION ENTITLED "SENDING AN ENCRYPTED ZIP FILE VIA EMAIL," MUST BE COMPLETED AND APPROVED AT TIME OF BID SUBMISSION; IF NOT, THE BIDDER MAY BE DECLARED NON-RESPONSIVE.

SECURITY REQUIREMENTS: Protection of Confidential Information:

(a) The contractor shall restrict access to all confidential information obtained from the Social Security Administration in the performance of this contract to those 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 at the postaward conference between the Contracting Officer and the responsible contractor representative.

(b) The contractor shall process all confidential information obtained from SSA in the performance of this contract under the immediate supervision and control of authorized personnel and in a manner that will protect the confidentiality of the records in such a way that unauthorized persons cannot retrieve any such records.

(c) The contractor shall inform all personnel with access to the confidential information obtained from SSA in the performance of this contract of the confidential nature of the information and the safeguards required to protect this information from improper disclosure.

(d) For knowingly disclosing information in violation of the Privacy Act, the contractor and the contractor employees may be subject to the criminal penalties as set forth in 5 U.S.C Section 552a (i)(1), which is made applicable to contractors by 5 U.S.C. 552a (m)(1) to the same extent as employees of the 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's employees may also be subject to the criminal penalties as set forth in that provision.

(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 Contractor Personnel Security Certification, Form SSA-301 (see **Exhibit A**). A copy of this signed certification must be forwarded to: SSA, Printing Management Branch (see **Exhibit K**).

(f) All confidential information obtained from SSA for use in the performance of this contract shall, at all times, be stored in an area that is physically safe from unauthorized access.

(g) 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 handled as confidential and may not be disclosed without the written permission of SSA. 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.

(h) The Government reserves the right to conduct on-site visits to review the contractor's documentation and in-house procedures for protection of confidential information.

(i) If a subcontractor is used for the sorting and/or mailing of the notices of this contract, the subcontractor must conform to all security requirements of the contract.

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. Further information may be found at: http://www.gsa.gov/portal/category/102371. 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 800-53 Rev4 before SSA provides data.

f. All ESPs that process or store Personally Identifiable Information (PII) 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) created by an independent assessor. 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 for more information on the Security Authorization Package.

***NOTE**: PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.*

***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.

For additional security requirements and NIST 800-53, REV 4 organization defined parameters, refer to "ESP Additional Security Controls Document."

References - Refer to most up to date revision:

- 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."

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

- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004.
  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

  and

  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 199, 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 200, 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 800-18, Guide for Developing Security Plans for Federal Information Systems, February 2006.
  https://doi.org/10.6028/NIST.SP.800-18r1

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

- ITL Bulletin Contingency Planning for Information Systems NIST Special Publication (SP) 800-34, Rev. 1.
  https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2010-07.pdf

- NIST SP 800-37 Revision 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, National Institute of Standards and Technology Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002.
  https://csrc.nist.gov/publications/detail/sp/800-47/final

- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.
  https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

- NIST SP 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, December 2014.
  https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final

- NIST SP 800-60 Volume 1 Revision 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

  and

  NIST SP 800-60 Volume 1 Revision 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-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007.
  https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

See **Exhibit B**, "SSA External Service Provider Additional Security Requirements" for complete details regarding this requirement.

Templates for Required Security Documents:

- **Exhibit C**: Security Assessment Report (SAR) Template
- **Exhibit D**: Risk Assessment Report (RAR) Template
- **Exhibit E**: System Security Plan (SSP) Template

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: It is the contractor's responsibility to properly safeguard personally identifiable information (PII) from loss, theft, or inadvertent disclosure and to immediately notify the Government of any loss of personally identifiable information.

PII is "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." (Ref.: OMB Memorandum 07-16) Other specific examples of PII include, but are not limited to:

(a) Personal identification number, such as passport number, driver's license number, taxpayer identification number, or financial account or credit card number;

(b) Address information, such as street address or personal email address; and,

(c) Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), fingerprints, handwriting, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry).

***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 logoff 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.
- Are prohibited from having any mobile devices or cameras in sensitive areas that contain any confidential materials. This includes areas where shredding and waste management occurs.

Managers at the contractor's facility working on this contract must also:

- 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 personally identifiable information 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 personally identifiable information. 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 breakroom 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 personally identifiable information 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.

Whenever the contractor's employee has doubts about a specific situation involving their responsibilities for safeguarding PII, they should consult GPO and/or SSA.

SECURITY AND SUITABILITY REQUIREMENTS FOR GOVERNMENT PRINTING (NOV 2018):

***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. The terms "vendor" and "contractor" are used interchangeably throughout this contract. Additionally, the terms "business days" and "workdays" are used interchangeably throughout this contract.*

(a) Suitability Process

The background investigation and adjudication processes are compliant with 5 CFR 731 or equivalent. Any new vendor personnel (i.e., those who have not previously received a suitability determination under this contract) requiring access to an SSA facility, site, information, or system, must complete and submit, through the COR-COTR, the documents listed in (a)(1) at least **30 workdays** prior to the date vendor personnel are to begin work. The suitability process cannot begin until the vendor submits, and SSA receives, accurate and complete documents.

(1) Suitability Document Submission

a. Immediately upon award, the Company Point of Contact (CPOC) must provide to the Center for Suitability and Personnel Security (CSPS) and a copy to the Contracting Officer's Representative (COR) for all vendor personnel requesting a suitability determination using a secured/encrypted email* with a password sent separately to dchr.ope.suitability@ssa.gov:

(i) An e-QIP applicant listing including the names of all vendor personnel requesting suitability;
(ii) Completed Optional Form (OF) 306, Declaration for Federal Employment (see **Exhibit F**);
(iii) Work authorization for non-United States (U.S.) born applicants, if applicable.

b. The e-QIP applicant listing must include the vendor name, the Social Security Administration (SSA) vendor number, the CPOC's name, the CPOC's contact information, the COR's name, the COR's contact information, and the full name, Social Security Number, date of birth, place of birth (must show city and state if born in the U.S. OR city and country if born outside of the U.S.), and a valid email address for all vendor personnel requesting suitability. All spelling of names, email addresses, places, and numbers must be accurate and legible.

(2) e-QIP Application

a. Once SSA receives all completed documents, listed in (a)(1), the Center for Suitability and Personnel Security (CSPS) will initiate the e-QIP process using the e-QIP applicant listing. CSPS will email the e-QIP notification to the CPOC and COR inviting vendor personnel to the e-QIP website to electronically complete the background investigation form (Standard Form (SF) 85P, Questionnaire for Public Trust Positions). (See **Exhibit G**.)

b. Vendor personnel will have up to 10 business days to complete the e-QIP application. The 10-day timeframe begins the day CSPS sends the invitation to the CPOC and COR. Vendor personnel must electronically sign the signature pages before releasing the application in e-QIP. Signature pages include the Certification, Release, and Medical Release pages for the SF 85P. Find information about the e-QIP process in the e-QIP Quick Reference Guide for e-QIP Applicants at https://nbib.opm.gov/e-qip-background-investigations/.

c. If vendor personnel need assistance with e-QIP logon and navigation, they can call the e-QIP Hotline at 1-844-874-9940.

(3) Fingerprinting

a. The e-QIP notification email also provides vendor personnel with instructions to obtain electronic fingerprinting services. Vendor personnel must report for fingerprint services immediately upon completion and release of the e-QIP application and within 10 business days from the day CSPS sends the invitation.

b. If vendor personnel cannot report to the designated fingerprint locations (in the notification email), CSPS will accept completed Field Division (FD) 258 fingerprint cards. (See **Exhibit H**.) The COR can provide the FD 258, if required. Vendor personnel must complete all fields on the FD 258. Incomplete fields may delay suitability processing.

c. If the vendor needs to mail completed FD 258 fingerprint cards, the vendor can send them, via certified mail, along with a completed Vendor Personnel Suitability Cover Sheet to: Social Security Administration Center for Suitability and Personnel Security, Attn: Suitability Program Officer, 6401 Security Boulevard, 2246 Annex Building, Baltimore, MD 21235.

(4) Status Check

If vendor personnel have completed each of the steps in (e) 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.

(b) Suitability Determination

(1) CSPS uses a Federal Bureau of Investigation fingerprint check as part of the basis for making a suitability determination.

This determination is final unless information obtained during the remainder of the full background investigation, conducted by the Office of Personnel Management, is such that SSA would find the vendor personnel unsuitable to continue performing under this contract. CSPS will notify the CPOC and the COR of the results of these determinations.

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

(3) If personnel have been cleared at a previous contractor's facility and are to perform work under a new vendor, the CPOC must submit a fully completed, legible Contractor Personnel Rollover Request Form to the COR. (See **Exhibit I**.) CSPS will notify the CPOC, COR, and Contracting Officer (CO) of suitability to work under the new vendor.

(c) Vendor Personnel Previously Cleared by SSA or Another Federal Agency

If vendor personnel previously received a suitability determination from SSA or another Federal agency, the CPOC should include this information next to the vendor personnel's name on the initial applicant listing (see paragraph (a)(1)(b)) along with the OF 306. CSPS will review the information. If CSPS determines another suitability determination is not required, it will provide a letter to the CPOC and the COR indicating the vendor personnel were previously cleared under another Federal contract and do not need to go through the suitability determination process again.

(d) Unsuitable Determinations

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

(2) The vendor 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. Vendor personnel must file their own requests; vendor may not file requests on behalf of vendor personnel.

dchr.ope.suitclarify@ssa.gov

OR

Social Security Administration; Center for Suitability and Personnel Security, Attn: Suitability Program Officer, 6401 Security Boulevard, 2246 Annex Building, Baltimore, MD 21235

(e) Vendor Notification to Government

The vendor shall notify the COR and CSPS within one business day if any vendor personnel are arrested or charged with a crime, or if there is any other change in the status of vendor personnel (e.g., leaves the company, no longer works under the vendor, the alien status changes, etc.) that could affect their suitability determination.

The vendor must provide in the notification as much detail as possible, including, but not limited to: name(s) of vendor personnel whose status has changed, SSA vendor number, the type of charge(s), if applicable, date of arrest, the court date, jurisdiction, and, if available, the disposition of the charge(s).

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 an 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(s)
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, personnel, production, and security control plans as required by this specification.

The contractor must demonstrate the capability to perform the requirements of the contract at time of award. 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 at least 90 calendar days prior to the start of live production on December 1, 2021.

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 plans, the contractor must submit updated plans within **two (2) workdays** of request.

Five (5) additional workdays will be permitted to provide a Security Assessment Package as required. The contractor, at SSA's discretion, may be granted **five (5) additional workdays** if additional information is required for the Security Assessment Package. The workday after notification to submit will be the first day of the schedule.

Option Years*:* For each option year that may be exercised, the contractor will be required to review their production plans and re-submit in writing the above plans detailing any changes and/or revisions that may have occurred. The revised plans are subject to Government approval. The revised plans 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.

PLEASE NOTE: The specifications in this contract cover the workloads of this contract transmitted daily and weekly. As such, the four (4) workloads of 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.

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-responsive.

Due to PII issues, the Government cannot award the contract until all security requirements are met. If the contractor fails to meet these requirements within **60 workdays** of start of live production, the contractor will be declared nonresponsive.

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 the products required under this specification 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 locations for a period longer than **five (5) workdays**, contractor must have a backup facility with the capability of producing the products required under this specification.

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, and a timetable for the start of production at that facility.

Part of the plan must also include the transportation of Government materials from one facility to another. SSA has the option to install a data connection into the contractor's backup facility.

NOTE: All terms and conditions of this contract will 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 shall provide and maintain, within their own organization, an independent quality assurance organization of sufficient size and expertise to 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 shall 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 shall 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 plan must account for the number of pieces mailed daily and must also cover the security over the postage meters as well as the controls for the setting of the meters (if meters will be used).

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, provide for backup and re-running in the event of an unsatisfactory sample, and contain control systems that will detect defective, missing, or mutilated pieces.

The plan should include the sampling interval the contractor intends to utilize. The contractor will be required to create two (2) control samples every 4,000 notices. The samples 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 task order and shipped to SSA, Printing Management Branch (see **Exhibit K**).

NOTE: Mailers with low volumes (less than 4,000) will require at least one (1) set of samples to be produced.

The plan shall detail the actions to be taken by the contractor when defects, 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 shall monitor all aspects of the job, including material handling and mail flow, to assure that 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.

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 notice 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 shall demonstrate the contractor's ability to provide complete hardware and software compatibility with SSA's existing network (see "PREPRODUCTION TESTS, *Transmission Test*" for additional information). The contractor must complete a System Plan (see **Exhibit J**).

Included with the Computer System Plan shall 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, a resume must still be included. This plan must show that the programmer(s) is skilled in the handling and programming of Advanced Function Presentation (AFP) (Fully Composed or Mixed Mode) printing platform.

Mail Plan – This plan should include sufficient detail as to how the contractor will comply with all applicable U.S. Postal Service (USPS) 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 presort postal discounts as outlined in the contract.

Material Handling and Inventory Control – This plan should explain in detail how the following materials will be handled: incoming raw materials; work-in-progress materials; quality control inspection materials; USPS inspection materials; and all outgoing materials cleared for USPS pickup/delivery.

Personnel Plan – This plan should include a listing of all personnel who will be involved with this contract. For any new employees, the plan should include the source of these employees and a description of the training programs the employees will be given to familiarize them with the requirements of this program.

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

(1) list of all production equipment and equipment capacities to be utilized on this contract;
(2) the production capacity currently being utilized on this equipment;
(3) capacity that is available for these workloads; and,
(4) if new equipment is to be utilized, documentation of the purchase order, source, delivery schedule, and installation dates are required.

The last leaf of the SSA-L732-OP1 notice within the eRPA data files contains a micro-perforated payment stub. (For Bilingual (Spanish/English) notices, the payment stub will be on the last leaf of both the Spanish and the English notices. However, the micro-perforated payment stub will not be on the same page for every notice because these notices have variable page counts.) The contractor will be required to identify the payment stub page(s) (English or Spanish/English) requiring perforation. Regarding the "select-a-perf" requirement, the contractor's production plan must explain how they will handle imaging and collating the required micro-perforated sheet into the proper sequence of leaves. The plan must also detail how the contractor intends to meet the critical margins associated with the scanline. (See "PRINTING/IMAGING.")

The contractor must disclose in their production plan their intentions for the use of any subcontractors. If a subcontractor will be handling SSA notices, 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 shall 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.
(3) How all applicable Government-mandated security/privacy/rules and regulations as cited in this contract shall 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) (see **Exhibit M**). Additional information is also available at: http://www.gsa.gov/portal/category/102371.

(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 Rev. 4. The SAP should be completed by either an independent assessor or another Federal agency.

Materials – The contractor is required to explain how all accountable materials will be handled throughout all phases of production.

Production Area Plan - The contractor must provide a secure area(s) dedicated to the processing and storage of data for the EAD, YCER, BEVE and eRPA 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) shall be limited to security-trained employees involved in the production of the notices.

Part of the Production Area Plan shall 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 (ex., 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 1/4 inch. All documents to be destroyed cannot leave the security of the building and must be destroyed by the contractor at contractor's printing site. The contractor must specify the method planned to dispose of the material.

UNIQUE IDENTIFICATION NUMBER: Unique identification 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 AFP 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, their 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 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 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 and inserts. 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 United States postal system.

Contractor must have all hardware, programming, and finalized reports in place to meet this requirement. The equipment must arrive 90 calendar days prior to the start of live production on December 1, 2021. 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 must 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 must be defined as follows:

- All notices received from SSA for each file date were printed, inserted, and entered correctly into the United States 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 with the correct inserts 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 piece that is 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, re-scanned, 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 ensures 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, 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 for 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 a 6-month period 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 time 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 (i.e., inserted, diverted, and reason for divert 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 (see **Exhibit L**, "Audit and Summary Reports").

(j) Contractor must generate a final automated 100% accountability summary report for each print order. This information must be generated directly from the audit report; manual inputs are not allowed.

The summary report must contain the following (see **Exhibit L**):

1. Job name.
2. Print order (must show sequence numbers for each section (i.e., first pass and then reprints).
3. Sequence number range for each print order and/or mail date.
4. Volume of all sequence numbers associated with the print order and or mail date were inserted.
5. Volume of reprints that were inserted for each print order and/or mail date.
6. Volumes for each file or print order and date that each was completed.

A PDF copy of the summary report(s) and matching USPS 3607R, and/or GPO 712 form(s) must be submitted to SSA, Printing Management Branch (see **Exhibit K**), for each file date within **two (2) workdays** of mailing.

Contractor must submit a sample of their Audit and Summary reports (see **Exhibit L)** with the required preaward production plans for 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.

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.

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.

NOTE: The Government will not as a routine matter request that 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 NOTICES PULLS FROM PRODUCTION: Due to the sensitivity of notices in this contract, the Government may request that the contractor remove individual notices from the production stream. When this occurs, the Government will supply the contractor with a list of Social Security Numbers (SSNs) or ID Codes that need to be pulled. The SSNs for each notice are contained in the Mail Run Data (MRD) File (see **Exhibit O**).

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.

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 one desk, one swivel arm chair, telephone lines, internet access via wireless or Ethernet for two computers, two work tables, and two 4-drawer letter-size files with combination padlock and penda-flex 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 any and all 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, 6401 Security Boulevard, Baltimore, MD, 21235, 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 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 the U.S. Postal Service. The contractor must present and explain their final plan for both printing, imaging, folding, inserting, and mailing the EAD, YCER**,** BEVE, and eRPA Notices. 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 shall meet with SSA and USPS representatives to present and discuss their plan for mailing. The preproduction meeting will include a visit to the contractor's mailing facility where the contractor is to furnish specific mail.

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.

ASSIGNMENT OF JACKETS, PURCHASE, TASK, AND PRINT ORDERS: A GPO jacket number will be assigned and a purchase order issued to the contractor to cover work performed. The purchase order will be supplemented by an individual daily "Task Order" for each job placed with the contractor. A print order will be issued weekly and will indicate the total number of task orders placed and the total number of notices produced that week. The print order will also indicate any other information pertinent to the particular order.

ORDERING: Items to be furnished under the contract shall be ordered by the issuance of weekly print orders supplemented by daily electronic task orders. Orders may be issued under the contract from **September 1, 2021** through **August 31, 2022**, plus for such additional period(s) as the contract is extended. All print orders and task 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 task order.

Task orders will be issued daily for purposes of the contract and shall detail the daily volume of notices required. A print order will be used for billing purposes, will be issued weekly, and will cover all daily task orders issued that week. A task order or print order shall be issued upon notification by the Government 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 shall 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) workloads consisting of English only and Bilingual (Spanish/English) personalized notices, business reply mail (BRM) envelopes, courtesy reply mail (CRM) envelopes, and mail-out envelopes, requiring such operations as: the receipt and processing of transmitted data; redevelopment of Advanced Function Presentation (AFP) (Fully Composed or Mixed Mode) printing platform; composition; printing and imaging; binding; construction; inserting and packing; manifesting and/or metering; and, distribution.

TITLE: EAD, YCER, BEVE, and eRPA Notices.

The four (4) workloads are as follows:

1. EAD (Earnings After Death)
2. YCER (Young Children's Earnings)
3. BEVE (Benefit Verification)
4. eRPA (Electronic Representative Payee Accounting System)

Future Workloads (during term of contract): During the term of this contract the Government expects to develop new notice workloads with the same requirements as the four (4) notice workloads described by these specifications. All terms and conditions in this specification will apply to these 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.

FREQUENCY OF ORDERS:

EAD and YCER Workloads: Electronic task order will be issued weekly (the morning after the transmission).
BEVE and eRPA Workloads: Electronic task order will be issued daily (Tuesday through Saturday).

Task orders will be issued the morning after the transmission with the volumes for notices, leaves, pages, and any insert required.

A print order will be issued weekly.

Separate print orders will be issued for the composition and proofs and for the preproduction validation tests.

QUANTITY: The combined total for EAD, YCER, BEVE, and eRPA notices is approximately 7,538,240 per year.

The Government reserves the right to increase or decrease by up to 25% of the total number of notices ordered annually.

NUMBER OF PAGES:

Notices: 1 to 20 printed pages (1 to 10 leaves) per notice.
All Envelopes: Face and back (after manufacturing).

TRIM SIZES:

EAD and YCER:

Notices: 8-1/2 x 11".
White CRM Envelope: 5-3/4 x 8-3/4", plus flap.
Window Mail-Out Envelope: 6-1/8 x 9-1/2", plus flap.

BEVE:

Notices: 8-1/2 x 11".
Window Mail-Out Envelope: 4-1/8 x 9-1/2", plus flap.

eRPA:

Notices: 8-1/2 x 11".
White BRM Envelope: 5-3/4 x 8-3/4", plus flap.
Green BRM Envelope: 3-7/8 x 8-7/8", plus flap.
Window Mail-Out Envelope: 6-1/8 x 9-1/2", plus flap.

MAKE-UP OF MAILERS: A record will be transmitted for each mailing address. The records will contain all the data relevant for the mailing of an associated mail piece. Unique alpha/numeric identifiers will be part of the record to ensure accuracy in the insertion process. All files transmitted by SSA will be physical sequential Advanced Function Presentation (Fully Composed or Mixed Mode) printing platform. Any alteration of the notice content in the file is not permitted.

FOR QUALITY CONTROL AND AUDITING PURPOSES: The contractor must not merge file dates and mailers during processing, printing, and mailing. Any alteration of the notice content in the file is not permitted.

The figures indicated below are estimates that are based on historical data of past production runs. The figures show the minimum and maximum quantities required daily, as well as the number of printed pages in a notice (notices are duplex printed and one-side only when an odd page is required), inserts (items that are to be inserted into the mail-out envelope along with the 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**.

MAKE-UP OF NOTICE MAILERS:

EAD: The EAD mailers are divided into three (3) notice categories by file names. All EAD notices consist of 1 or 2 pages and a mail-out envelope, and may require a White CRM envelope.

Mailer 1 (EADER):

Transmission Minimum:	0
Transmission Maximum:	28,270
Leaves:	1
Printed Pages:	2
	Personalized Notice (Form SSA-L4112-C1)
	Mail-out Envelope (6-1/8 x 9-1/2")
Inserts:	White CRM Envelope
Folding:	Bifold

Mailer 2 (EADEE):

Transmission Minimum:	0
Transmission Maximum:	45,597
Leaves:	1
Printed Pages:	1
	Personalized Notice (Form SSA-L3044-C1)
	Mail-out Envelope (6-1/8 x 9-1/2")
Inserts:	None
Folding:	Bifold

Mailer 3 (EADSE):

Transmission Minimum:	0
Transmission Maximum:	26
Leaves:	1
Printed Pages:	1
	Personalized Notice (Form SSA-L3400-C1)
	Mail-out Envelope (6-1/8 x 9-1/2")
Inserts:	None
Folding:	Bifold

YCER: The YCER mailers are divided into three notice categories by file names. ALL YCER notices consist of 1 or 2 pages and a mail-out envelope, and may require a White CRM envelope.

Mailer 4 (YCERER):

Transmission Minimum:	0
Transmission Maximum:	5,016
Leaves:	1
Printed Pages:	2
	Personalized Notice (Form SSA-L3231-C1)
	Mail-out Envelope (6-1/8 x 9-1/2")
Inserts:	White CRM Envelopes
Folding:	Bifold

Mailer 5 (YCEREE):

Transmission Minimum:	0
Transmission Maximum:	9,239
Leaves:	1
Printed Pages:	1 or 2
	Personalized Notice (Form SSA-L3232-C1)
	Mail-out Envelope (6-1/8 x 9-1/2")
Inserts:	None
Folding:	Bifold

Mailer 6 (YCERSE):

Transmission Minimum:	0
Transmission Maximum:	189
Leaves:	1
Printed Pages:	1
	Personalized Notice (Form SSA-L3241-C1)
	Mail-out Envelope (6-1/8 x 9-1/2")
Inserts:	None
Folding:	Bifold

BEVE: The BEVE mailer is one notice consisting of 1 to 3 pages and a mail-out envelope (P.O. Box 31500).

Mailer 7

Transmission Minimum:	15,000
Transmission Maximum:	40,000

Leaves:	1 or 2
Printed Pages:	1 to 3
	Personalized Notice (No form number)
	Mail-out Envelope (4-1/8 x 9-1/2”)
Inserts:	None
Folding:	Trifold

eRPA:

The eRPA mailer consists of four (4) notice types transmitted in one file. These personalized notices are English ONLY (Mailer 8) and Bilingual (Spanish/English) (Mailer 9) and range from 1 to 20 pages (1 to 10 leaves). An occasional mailer (less than 1%) may exceed these leaf counts.

All eRPA notices require a mail-out envelope. Form SSA-L732 requires a White BRM envelope; Form SSAL732-OP1 requires both a White and a Green BRM envelope.

The Redirect Notices and Call-In Notices DO NOT REQUIRE any BRM envelopes.

Mailer 8:

Transmission Minimum:	0
Transmission Maximum:	12,756
Leaves:	1 to 10
Printed Pages:	1 to 20
	Personalized English Notice (Form SSA-L732)
	Personalized English Notice (Form SSA-L732-OP1)*
	Redirect English Notice (No Form Number/No Inserts)
	Call-In English Notice (No Form Number/No Inserts)
	Mail-out Envelope (6-1/8 x 9-1/2”)
Inserts:	White BRM Envelope (Form SSA-L732/ Form SSA-L732-OP1)
	Green BRM Envelope (Form SSA-L732-OP1 only)
Folding:	Bifold

Mailer 9:

Transmission Minimum:	0
Transmission Maximum:	221
Leaves:	1 to 10
Printed Pages:	1 to 20
	Personalized Bilingual (Spanish/English) Notice (Form SSA-L732)
	Personalized Bilingual (Spanish/English) Notice (Form SSA-L732-OP1)*
	Call-In Bilingual (Spanish/English) Notice (No Form Number/No Inserts)
	Mail-out Envelope (6-1/8 x 9-1/2”)
Inserts:	White BRM Envelope (Form SSA-L732/ Form SSA-L732-OP1)
	Green BRM Envelope (Form SSA-L732-OP1 only)
Folding:	Bifold

New Notice Workloads:

Mailers 10, 11, and 12:

Minimum:	0
Maximum:	35,000

Leaves:	1 to 10
Printed Pages:	1 to 20 English Notices or Bilingual (English/Spanish) Notices Mail-out Envelope (4-1/8 x 9-1/2" or 6-1/8 x 9-1/2")
Inserts:	Variable When required, Reply Envelope
Folding:	Trifold or Bi-fold

PAYMENT STUB NOTE:

Form SSA-L732-OP1 Payment Stub Requirement: The next to the last leaf of the English ONLY Notice and the next to the last leaf of both the Spanish and the English Notices of the Bilingual Notice require a full horizontal micro-perforation, 3-1/2" up from bottom of page, along the entire 8-1/2" length dimension. However, the micro-perforated payment stub will not be on the same page for every notice because these notices have variable page counts.) The contractor will be required to identify the payment stub page(s) (English or Spanish/English) requiring perforation.

NOTE: The eRPA bilingual notices require insertion of both a Spanish and English notice in one envelope. On occasion, an eRPA mailer (10 leaves maximum) will exceed one ounce in weight.

The payment stub page (full 8-1/2 x 11" leaf) is part of the notice itself and will be electronically transmitted.

FILE NAME	MAILER	DATA SET NAME
EAD	Mailer 1	EERAFP.M10*orderid.Ryymmdd*
	Mailer 2	EEEAFP.M20*orderid.Ryymmdd*
	Mailer 3	ESEAFP.M30*orderid.Ryymmdd*
YCER	Mailer 4	YERAFP.M40*orderid.Ryymmdd*
	Mailer 5	YEEAFP.M50*orderid.Ryymmdd*
	Mailer 6	YSEAFP.M60*orderid.Ryymmdd*
BEVE	Mailer 7	BEVAFP.M70*orderid.Ryymmdd*
eRPA	Mailer 8 (English)	RPAAFP.M8*orderid.Ryymmdd*
	Mailer 9 (Spanish/English)	RPAAFP.M9*orderid.Ryymmdd*

Vendor – is the identifier. This is assigned when the transmission connectivity is installed.
aaaaa – is the order ID assigned by Control M at run time. This is used to build the unique identifier for the file.
yymmdd – is the year, month, and day of the file being transmitted. This is also referred to as the run date.

NEW NOTICES: The file names/dataset names for each new notice workload will be supplied to the contractor as they are developed.

CRM ENVELOPES:

EAD:

White CRM Envelopes (5-3/4 x 8-3/4")	90-Calendar Day Estimated Volumes
Wilkes Barre Direct Operations Center P.O. Box 80 Wilkes Barre, PA 18767-0080	27,883

YCER:

White CRM Envelopes (5-3/4 x 8-3/4")	90-Calendar Day Estimated Volumes
Wilkes Barre Direct Operations Center P.O. Box 40 Wilkes Barre, PA 18767-0040	4,940

BRM ENVELOPES:

eRPA:

White BRM Envelopes (5-3/4 x 8-3/4")	90-Calendar Day Estimated Volumes
Wilkes Barre Direct Operations Center P.O. Box 8500 Wilkes Barre, PA 18767-9998	204,223

Green BRM Envelopes (3-7/8 x 8-7/8")	90-Calendar Day Estimated Volumes
Mid-Atlantic Program Service Center P.O. Box 3430 Philadelphia, PA 19122-9985	3,712

NOTE: The contractor must submit billing invoice for all surplus inventory within 90 calendar days of completion of the contract in order to receive payment.

MAIL-OUT ENVELOPES:

Bifold Size: 6-1/8 x 9-1/2"		90-Calendar Day Estimated Volumes
EAD:	Wilkes Barre Direct Operations Center P.O. Box 80 Wilkes Barre, PA 18767-0080	27,883
YCER:	Wilkes Barre Direct Operations Center P.O. Box 40 Wilkes Barre, PA 18767-0040	4,940

Trifold Size: 4-1/8 x 9-1/2"		90-Calendar Day Estimated Volumes
BEVE:	Northeaster Program Service Center P.O. Box 315100 Jamaica, NY 11431-4089	1,625,000

Bifold Size: 6-1/8 x 9-1/2"		90-Calendar Day Estimated Volumes
eRPA:	Wilkes Barre Direct Operations Center P.O. Box 8500 Wilkes Barre, PA 18767-8500	206,884

GOVERNMENT TO FURNISH:

Manuscript copy for eight (8) envelopes, as follows:

- three (3) mail-out envelopes (6-1/8 x 9-1/2")
- one (1) mail-out envelope (4-1/8 x 9-1/2")
- two (2) White CRM envelopes (5-3/4 x 8-3/4")
- one (1) White BRM envelope (5-3/4 x 8-3/4")
- one (1) Green BRM envelopes (3-7/8 x 8-7/8")

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

At the Government's option, camera copy or electronic files (PostScript format) for the recycled paper logo and legend may be furnished for the notices and envelopes. Electronic files will be furnished via email.

PS Form 3615, Mailing Permit Application and Customer Profile Postage and Fees Paid Mailing Indicia.

A data connection between the contractor's specified location and the nearest available SSA network interface location or SSA's National Computer Center.

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: SSA External Service Provider Additional Security Requirements
Exhibit C: Security Assessment Report (SAR) Template
Exhibit D: Risk Assessment Report (RAR) Template
Exhibit E: System Security Plan (SSP) Template
Exhibit F: Declaration for Federal Employment (Optional Form 306)
Exhibit G: Questionnaire for Public Trust Positions (Standard Form (SF) 85P)
Exhibit H: Fingerprint Card (FD-258)
Exhibit I: Contractor Personnel Rollover Request Form
Exhibit J: System Plan
Exhibit K: Key SSA and GPO Personnel Contact Information
Exhibit L: Audit and Summary Reports
Exhibit M: 3PAO-Obligations-and-Performance-Guide v1.0
Exhibit N: Perforated Payment Stub
Exhibit O: Mail Run Data (MRD) File
Exhibit P: Postage Meter Activity Log

ELECTRONIC FILES:

All files will be electronically transmitted to the contractor and contain a complete record for each notice. Any programming or other format changes necessitated due to the contractor's method of production will be the full responsibility of the contractor and must be completed prior to SSA's validation. All files transmitted by SSA will be physical sequential Advanced Function Presentation (Fully Composed or Mixed Mode). Any alteration of the notice content in the file is not permitted. The contractor must not merge file dates and mailers (if applicable) during processing, printing/imaging, and mailing.

The contractor must not compress files in processing data for this contract.

The contractor will receive three (3) files for each print file: the Advanced Function Presentation (Fully Composed or Mixed Mode) printing platform, the Mail Run Data (MRD) file, and the Banner (BNR) file. The notice files for printing are formatted for the AFP printing platform in duplex printing (face and back). For proper processing of AFP, SSA supplies resources used for printing notices in AFP format. The MRD file will contain all information relevant to each mail piece. This would include, for each mail piece, the unique alpha/numeric identifier (the sequential number of the document), the number of sheets of paper, required inserts and insertion bin selection, recipient's address, return address, USPS IMB, the appropriate signature, and any required inserts. The BNR file contains information for setting up the intelligent inserters such as file totals, number of mail packets, and bin set up for those items being included in the mail packets and the total required in each bin.

The contractor will receive an electronic daily task order for BEVE and eRPA and weekly task order for EAD and YCER in the morning after transmission with the volumes for notices, leaves, pages, and any inserts required.

Whenever the contractor makes a change in the programming, the contractor will be required to execute a self-certification statement specifying the date of the last programming change. Prior notification of a programming change is required in addition to the self-certification statement for the contractor to schedule a validation test with SSA.

Prior to the commencement of production of orders placed under this contract, the Government will furnish preproduction electronic test files shortly after the postaward conference that are to be used in performing the various preproduction validation tests. Files will be in print image format and in ZIP Code sequence. Contractor will be required to sort files as necessary to obtain maximum USPS Postal discounts (i.e., leaf counts or mail weight).

Dataset names for the items listed below will be provided at the postaward conference or shortly thereafter:

Print Resource Library (AFP) for Transmission or email: AFP resources include page and form definitions, fonts, page segments, and overlays (if applicable) for page formatting.

Preproduction Press and Mail Run Test Files for Transmission: An AFP formatted print file with the corresponding MRD file and BNR file will be provided for each workload in the quantities required.

Revised Resource Library (AFP) for Transmission or Email (when applicable): AFP print resources, overlays, page segments, and non-standard fonts provided shortly after the postaward conference may change during the term of the contract, in which case a revised AFP resource file will be electronically transmitted to the contractor as a replacement.

PRINTER RESOURCES (AFP): SSA will provide the AFP (Fully Composed or Mixed Mode) resources for notice workloads. These resources will be provided to the contractor via transmission or email shortly after the postaward conference. SSA will also provide test files for transmission with samples of each workload to enable the start of the validation process.

The test files are to be used in the preproduction press and mail run test (see "PREPRODUCTION TESTS, *Preproduction Press and Mail Run Test"*).

These compliances relate solely to interpreting and printing files to be provided to the contractor by SSA, to ensure that the contractor is able to print the files as provided without alteration of any kind on the part of SSA. <u>It is solely the contractor's responsibility to re-develop/re-program the AFP (Fully Composed or Mixed Mode) resources and MRD file to ensure proper printing and inserting in their environment.</u>

NOTE: The AFP (Fully Composed or Mixed Mode) file contains all AFP resources, except licensed fonts, required to print this file.

The contractor will be responsible for maintaining the Advanced Function Presentation (AFP; Fully Composed or Mixed Mode) resources on each system that processes SSA's notices. SSA will provide updated resources electronically, as necessary.

When the contractor receives an update to the printer resources, the contractor will be required to provide SSA with 75 sample documents representative of the workload involved, from the test files, within **five (5) workdays** for review (see below). The contractor is to continue using existing resources while the samples are reviewed. Once the samples are approved, the contractor will be advised when to implement the new printer resource files into live production. Whenever testing is required, the contractor will be responsible for performing the test on each printer that processes SSA's notices.

The sample documents must be submitted as follows:

EAD and YCER Workloads:

- Submit 25 printed samples each to: SSA, Printing Management Branch (see **Exhibit K**).
- Submit 50 printed samples each to: SSA, Wilkes-Barre Direct Operations Center, Attn: EAD/YCER Analyst, Room 341, 1150 East Mountain Drive, Wilkes-Barre, PA 18702-7997.

eRPA Workloads:

- Submit 25 printed samples to: SSA, Printing Management Branch (see **Exhibit K**).
- Submit 50 printed samples to: SSA, Wilkes-Barre Direct Operations Center, Attn: eRPA Analyst, Room 341, 1150 East Mountain Drive, Wilkes-Barre, PA 18702-7997.

SSA's Printing Management (DMIM) will notify the contractor of these changes as soon as possible. Upon successful testing of the changes, SSA must transmit the new print resources (if necessary) and resume transmission of the notice file(s).

During the term of the contract, the Government anticipates making programmatic changes to the daily notices as warranted (e.g., changes in language, format, appearance, etc.). When changes occur, SSA will perform testing of the workload in their print facility for a short period of time. (The "Dark Days" for the contractor should only last a few days.) Only those affected workloads (indicated by filename) will be held back at SSA for validation and production. For example, if the BEVE notice workload were to be changed, SSA would test and print those notices only. The contractor would continue to print and mail the eRPA notice workloads. Upon successful testing of the changes by SSA, SSA will then transmit the new print resources (if necessary) and resume transmission of the notice file(s).

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

Contractor must have programmer(s) capable of handling AFP resources.

***Secure File Transfer Protocols (SFTP) Site**:* Contractor is required to set up, establish, and maintain a Secure File Transfer Protocol site that multiple users at SSA can access for passing PDF notice validation samples containing PII to SSA and back. Contractor cannot send PDF notices with PII via email.

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 under GSA's Networx contract to be installed within 60 to 90 calendar days 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 will 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 must provide adequate rack space for securing the router and firewall; the contractor must provide a dedicated analog dial-up line within eight (8) feet of the router. This dedicated analog dialup 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.

Upon contract award, the contractor must 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 must 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 persons 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 must be the HELP DESK at 877-697-4978.

FILE TRANSFER MANAGEMENT SYSTEM (FTMS) REQUIREMENTS: The contractor must provide the capability to interface with SSA's National FTMS for electronic transmission of designated 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, TIBCO's Managed File Transfer Platform Server. 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 its own name/address translation to fulfill the intended purpose of data transfers. SSA will provide Managed File Transfer node information to 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 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 Platform Server software's Checkpoint/Restart feature.

The contractor may not use VM/VSE/ESA on a mainframe system as this hinders automated file transmission.

The contractor's FTMS software must be operational for the receipt of data files 24 hours a day, seven (7) days a week, unless otherwise specified by the Government. The communications protocol between SSA and the contractor must be the Internet Protocol (IP). The contractor must specify the type 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 directed 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.

Transmission of production files must be the standard, automated technique. 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 connection problems arise and transmission cannot take place. SSA's first point of contact for systems or connectivity problems is the HELP DESK at (877) 697-4889.

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.

PREPRODUCTION TESTS: Prior to the commencement of production on the contract, the contractor will be required to demonstrate their ability to perform the contract requirements. The Government will furnish electronic test files at the postaward conference, or shortly thereafter, to be used in performing a Transmission Test, Preproduction Validation Test, a Payment Stub Validation Test, a Preproduction Press and Mail Run Test, and a Systems Change/Signature Change/New Notice Files Validation Test.

Failure of the contractor to perform any of the below tests satisfactorily may be cause for default. The Government reserves the right to waive the requirements of any of these tests. The contractor will be notified at the postaward conference if any test(s) is to 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.

When Preproduction Validation and/or Validation Tests are required, the Government will include them on a print order.

The contractor will be required to perform the following tests:

Transmission Test: Within one (1) week of the data connection being installed, the contractor will be required to receive within **one (1) workday** approximately 141,292 notices. Notices will be either 1 or 2 printed pages.

The contractor will be required to perform a record count verification (broken down by data set name) the same workday of the complete transmission of the test files and perform the Coding Accuracy Support System (CASS) certifications the same workday as receipt of the complete transmission of all notice test files. Additionally, the contractor must provide a timeline showing how long it took to receive the test files.

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

The contractor will be required to copy the files to their own system and provide to the SSA, Printing Management Branch (see Exhibit K) the exact counts received (broken down by data set name) before proceeding with any other processing.

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

When the record count verification and CASS certification have been successfully completed, the contractor will be required to process the test files and provide SSA, within **two (2) workdays**, 30 sample notices from each mailer from the transmission test files for EAD, YCER, BEVE, and eRPA workloads.

Contractor to submit these test samples to: SSA, Printing Management Branch (see Exhibit K).

The Government will approve, conditionally approve, or disapprove the samples from the Transmission Test 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.

NOTE: If errors are found, additional samples will be required until such time as the validation produces no errors.

***Preproduction Validation Test*:** Within **five (5) workdays** of receipt of test files and prior to the Preproduction Press and Mail Run Test, the contractor will be required to provide SSA, no less than 225 total samples of the completed product as specified below.

Notices must be complete and include all variable data from the Government furnished files and inserted into mail-out envelopes. Seal envelopes.

The Validation Test Samples are to be shipped in the following manner:

- Submit 25 printed EAD samples, 25 printed YCER samples, and 25 printed eRPA samples to: SSA, Printing Management Branch (see Exhibit K).

- Submit 50 printed EAD samples and 50 printed YCER samples to: SSA, Wilkes-Barre Direct Operations Center, Attn: EAD/YCER Analyst, Room 341, 1150 East Mountain Drive, Wilkes Barre, PA 18702-7997.

- Submit 50 printed eRPA samples to: SSA, Wilkes-Barre Direct Operations Center, Attn: eRPA Analyst, Room 341, 1150 East Mountain Drive, Wilkes Barre, PA 18702-7997.

The Government will approve, conditionally approve, or disapprove the preproduction validation test output within **five (5) 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.

If errors are found, additional samples of notices (as indicated above) will be required until such time as the validation produces no errors. All samples must be manufactured at the facilities and on the equipment in which the contract production quantities are to be manufactured**.**

If required due author's alterations or contractor's error, the contractor must submit revised samples within five (5) workdays of notification. The Government will approve, conditionally approve, or disapprove the preproduction validation test samples within **three (3) workdays** of receipt thereof.

Payment Stub Validation Test (eRPA OP1 only): Within **five (5) workdays** of receipt of test files and prior to the Preproduction Press and Mail Run Test, the contractor will be required to provide 100 printed samples of Form SSA-L732-OP1 containing a payment stub for validation of the scanline.

The micro-perforation on the payment stub page must be properly located and the payment stub must function properly when processed through the current high-speed scanning equipment owned by SSA. A form is a reject when its OCR print cannot be correctly deciphered on the first pass through the specified reading equipment.

Contractor to submit samples as follows:

- Submit 50 printed samples to: SSA/Wilkes-Barre Direct Operations Center, Attn: Patrice Gallagher, Room 341, 1150 East Mountain Drive, Wilkes Barre, PA 18702-7997.

- Submit 50 printed samples to: SSA, Printing Management Branch (Exhibit K).

The Government will approve, conditionally approve, or disapprove the preproduction validation test output within **five (5) 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.

Preproduction Press and Mail Run Test (24-Hour Test): Within **five (5) workdays** of receipt of test files and after the contractor receives the materials necessary to perform the test, the contractor will be required to demonstrate their ability to perform the contract requirements by performing a 24-hour preproduction press and mail run test utilizing the test files transmitted electronically.

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

The Government will issue a print order to the contractor 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 for the applicable line items in the "SCHEDULE OF PRICES." If the contractor fails to meet all test requirements, they will not be reimbursed for any associated costs.

Contractor must perform the preproduction press and mail run tests in a continuous 24-hour period, as required, that will prove to the Government representatives that the contractor can satisfactorily complete the requirements of this contract during live production.

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 beginning the test. Notices are to be completed in accordance with contract requirements, inserted with inserts into envelopes, and prepared for mailing.

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

The contractor must produce a minimum of 56,945 notices.

During the 24-hour period, the contractor will be required to print and prepare for mailing the following quantities of EAD, YCER, BEVE, and eRPA notices:

EAD	Mailer 1 (EADER)	4,039
	Mailer 2 (EADEE	6,514
	Mailer 3 (EADSE)	1
YCER	Mailer 4 (YCERER)	717
	Mailer 5 (YCEREE)	1,320
	Mailer 6 (YCERSE)	27
BEVE	Mailer 7	40,000
eRPA	Mailer 8 (English)	4,253
	Mailer 9 (Spanish/English)	74
TOTAL		56,945

The 24-hour period for the printing process will begin when an "O.K. to Print" is given by the Government representative on-site.

The 24-hour period for the inserting 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 press run test run will incorporate all aspects of the program consisting of the receipt of transmitted data; the duplex printing and imaging (and simplex printing/imaging when an odd page is required) of notices; gathering; folding; inserting; manifesting; metering (if approved by SSA under certain circumstances); presorting; and preparing finished notices for delivery to the USPS. (This must include any and all reprints required during the course of this test.) 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 EAD, YCER, BEVE, and eRPA Notice Preproduction Press and Mail Run Test on the equipment they intend to use during live production and using their personnel.

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 output within **seven (7) 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.

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

When required, contractor to submit samples within **five (5) workdays** of receipt of files.

The contractor shall furnish 100 total samples of the notices with the changes (no envelopes or inserts), as follows:

- Submit 25 printed samples to: SSA, Printing Management Branch (see Exhibit K).
- Submit 25 printed EAD samples and 25 printed YCER samples to: SSA, Wilkes-Barre Direct Operations Center, Attn: EAD/YCER Analyst, Room 341, 1150 East Mountain Drive, Wilkes Barre, PA 18702-7997.
- Submit 25 printed eRPA samples to: SSA, Wilkes-Barre Direct Operations Center, Attn: eRPA Analyst, Room 341, 1150 East Mountain Drive, Wilkes Barre, PA 18702-7997.

The Government will approve, conditionally approve or disapprove the samples within **seven (7) 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 Systems Change/Signature Change/New Notice Files Validation Test must occur without a break in production of daily notices. The Government will inform the contractor in advance when the regular daily transmissions will contain the systems changes.

COMPOSITION: Contractor will be required to set type for approximately 6 to 9 lines of type for eight (8) envelopes. Helvetica or similar typeface will be utilized.

Century Schoolbook or equivalent fonts (Sonoran Serif) are to be used for producing the notices.

SSA will not provide all required fonts to the contractor. Obtaining licensed fonts will be the responsibility of the contractor. SSA will provide the font part numbers to the contractor who will validate that they have the proper licenses for each required font.

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

Intelligent Mail Barcode font will be required during the term of the contract. The contactor will be required to obtain the necessary font; SSA will not provide it with resources supplied.

PROOFS (Envelopes Only): One (1) press quality PDF soft proof (for content only) using the same Raster Image Processor (RIP) that will be used to produce the final printed product may be required. PDF proof will be evaluated for text flow, image position, and color breaks. Proof will not be used for color match.

Proofs must show all margins and dimensions, indicate trim marks, and must show flap and window size/placement, as applicable.

SSA reserves the right to make changes to all proofs. The Government may require one or more sets of revised proofs before rendering an "O.K. to Print."

If any contractor's errors are serious enough in the opinion of 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.

Contractor must not print prior to receiving and "O.K. to Print."

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.

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

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

White BRM/CRM Envelopes (5-3/4 x 8-3/4"): White Writing Envelope, basis weight: 20 lbs. per 500 sheets, 17 x 22", equal to JCP Code V20. EXCEPTION: Stock must contain a minimum of 50 percent waste paper.

Green BRM Envelopes (3-7/8 x 8-7/8"): Green Writing Envelope (close match of Pantone 344), basis weight: 20 lbs. per 500 sheets, 17 x 22", equal to JCP Code V20. EXCEPTION: Stock must contain a minimum of 50 percent waste paper. **NOTE**: Surface Tinting of envelopes is not permitted.

Mail-Out Window Envelopes (4-1/8 x 9-1/2" and 6-1/8 x 9-1/2"): White Writing Envelope, basis weight: 24 lbs. per 500 sheets, 17 x 22", equal to JCP Code V20; or at contractor's option, White Uncoated Text, basis weight: 60 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60.

PRINTING/IMAGING: Contractor will be required to convert furnished data from electronic transmission for either laser or ion deposition printing. All imaging/printing must have a minimum resolution of 600 x 600 dpi. **NOTE**: Inkjet printing is NOT allowed.

The Government reserves the right to make changes to the envelopes 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. Therefore, the contractor is not to preprint or maintain more than a 90-calendar day surplus/inventory of any of the components required on this contract. The Government will not be required to purchase from the contractor the surplus/inventory of any component remaining on hand in excess of what was authorized when an envelope or format/text change is implemented.

Notices: All notices are simplex (face only) and/or duplex (face and back, head-to-head), printed/imaged in black ink. Notices can require a combination of simplex and duplex printing/imaging. Printing and imaging consist of text and line matter.

On the eRPA SSA-L732-OP1 Notices, leaves print both face only and face and back. The Verification Form, Payment Stub, and Privacy Act Statement portions each start printing on a face page. The Payment Stub and Privacy Act Statements are one page each and print face only.

The eRPA notices contain client completed notices that are read by OCR equipment. The notices (front and back) will be read by a Kodak document Scanner 9500, 9520, 1840, or other high-speed scanner. The format for these notices will be incorporated in the body of the notice and must be printed as specified below to be scanned.

For the eRPA only, the alpha-numeric scan line must be printed using the OCR A font. The OCR printing must read continuously on an Integrated Image Based Data Capture System (IIBDCS).

ANSI X3.17 "Character Set for Optical Character Recognition (OCR A)" must apply to these specifications. The revisions of this standard which are effective as of the date of this contract are those which must apply.

All Envelopes: Envelopes print face and back (after manufacture) in black ink. 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.

CRM Envelopes: Face of envelope to be in COURTESY REPLY FORMAT. Print FIMs and barcodes using the furnished camera copy. The FIMs and barcodes should be placed on the mailing piece according to the current U.S. Postal Service's Domestic Mail Manual, "Barcoded Mail Pieces."

BRM Envelopes*:* Face of envelope to be in BUSINESS REPLY MAIL FORMAT. Print FIMs and barcodes using the furnished camera copy. The FIMs and barcodes should be placed on the mailing piece according to the current U.S. Postal Service's Domestic Mail Manual, "Barcoded Mail Pieces."

NOTE: Inside of BRM envelopes must contain a clear area (no pantograph design), approximate 3-1/2 x 5/8" in size, behind the barcode to ensure the readability of barcode by the U.S. Postal Service equipment.

Mail-Out Envelopes: Mail-out envelopes require a security tint (lining is acceptable) printed on the inside (back - before manufacture) in black ink. 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.

2-Dimensional Barcodes: A 2-D barcode of SSA's choice (currently Data Matrix) must be imaged (minimum 600 x 600 dpi) at the bottom left on first two pages of EAD and YCER notices,

The Data Matrix barcode height and width is to be 5/8", plus or minus 1/16". **NOTE**: At least 1/8" margin (quiet zone) is required top, bottom, left, and right of each barcode.

Data columns are to be preceded and followed by the standard Data Matrix start/stop patterns, left row indicator, and right row indicator. Additionally, a delimiter character (comma) must be inserted between each element. The 2-D barcodes will encode 114 characters including the following data elements:

In each print file on the page where a 2-D barcode should be printed, there is a 5 A NOOP record. It can be identified by the string "2DBCDATA" beginning in column 10. The data for the barcode begins in column 18 (for a total length of 114) and the fields are as follows:

Form Type	length 4
Processing Year	length 2
Page Number	length 1
Sequence Number	length 12 (left justified)
EIN	length 9
Reported SSN	length 9
Reported Name:	
First Name	length 11 (left justified)
Middle Initial	length 1
Last Name	length 15 (left justified)
Earnings	length 11 (left justified)
Tax Year	length 4
Employer Name	length 35 (left justified)

NOTE: Personalized forms data to be included in the barcode will be contained in the SSA wire file transmissions.

The 2-D Data Matrix barcodes must be in accordance with the following ISO standards: ISO/IEC 16022 – "International Symbology Specification, Data Matrix;" ISO/IEC 15418:1999 – "Symbol Data Format Semantics;" ISO/IEC 15434:1999 – "Symbol Data Format Syntax;" and ISO/IEC 15415 – "Print Quality Standard."

1-Dimensional Barcodes: A barcode of SSA's choice (currently Code 39 - 3 of 9) must be imaged (minimum 600 x 600 dpi) at the bottom left on each printed/imaged page on all eRPA SSA-L732 Notices, approximately 1/4 inch below the OCR scan line. The Code 39 (3 of 9) barcode height is to be 1/4" (plus or minus 1/16"), and the width is to be 5" (plus or minus 1/8"). **NOTE**: At least 1/8" margin (quiet zone) is required top, bottom, left, and right of each barcode.

The (3 of 9) barcodes must be in accordance with ANSI MH 10.8M-1983, unless otherwise specified.

NOTE: Personalized forms data to be included in the barcode will be contained in the SSA file transmissions.

All barcodes will be tested for scannability on the below specified equipment at the SSA, Wilkes-Barre Data Operations Center in Wilkes-Barre, PA.

The forms produced under these specifications must be guaranteed to function properly when processed through Kodak High Speed 9500, 9520, 1840 or other high-speed Scanners. SSA will be using Top Image Systems scanning software to process the images; OCR engines to do the ICR; and, an Inlite Engine to read the barcodes. Forms require precision spacing, printing, trimming and folding. OCR forms will be extracted from CRM/BRM using the following equipment: OPEX MPE 7.5 Multiple Purpose Extractor.

RECYCLED PAPER LOGO: If recycled paper is used, the recycled paper logo and legend must be printed in black ink on the notices and envelopes. The recycled paper logo/legend must be digitized by the contractor and imaged in the bottom left corner of notices aligned with the contractor's control number on the first page of each notice and imaged on the back of the envelopes.

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. When a press sheet inspection is required, it will be specified on the individual print order 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.

Press sheets must contain control bars for each color of ink on the sheet. Control bars must be placed parallel to the press's ink rollers. The control bars (such as BRUNNER, GATF, GRETAG, or RIT) must show areas consisting of 1/8 x 1/8" minimum solid color patches; tint patches of 25, 50, and 75%; dot gain scale; and gray balance patches for process color (if applicable). These areas must be repeated across the entire press sheet.

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: Before production begins on any new workloads, a press sheet inspection may be required at the contractor's plant.

MARGINS: Margins will be as indicated on the print order, furnished copy, or furnished electronic file.

NOTE: Notices must appear exactly as approved during validation. Absolutely no deviation will be accepted.

BINDING:

Notices: Trim four sides.

Payment Stub: For the eRPA notices, the next to the last leaf of the English ONLY Notice and the next to the last leaf of both the Spanish and the English Notices of the Bilingual Notice will contain a micro-perforated payment stub. However, the micro-perforation will not be on the same leaf for every notice because the notices have variable page counts. The contractor will be required to identify the payment stub page(s) requiring perforation and ensure that only these pages are perforated.

Perforation - It is critical that the micro-perforation on the payment stub page must be 3-1/2" (plus or minus 1/16") from the bottom of the payment stub page and run along the entire 8-1/2" dimension (see **Exhibit N**).

CONSTRUCTION:

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

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

Green BRM Envelope (3-7/8 x 8-7/8"): Envelope must be open side, with gummed, fold-over flap for sealing and contain high-cut diagonal or double side seams, at contractor's option. Flap depth is at the contractor's option but must meet all USPS requirements. Flap must be coated with suitable remoistenable glue that will securely seal the return envelope for mailing. Adhesive must not adhere to the contents of the envelope.

EAD and YCER Mail-Out Envelope (6-1/8 x 9-1/2"): Envelope must be open side, with gummed, fold-over flap for sealing and contain high-cut diagonal seams or double side seams, at contractor's option. Flap depth is at the contractor's option but must meet all USPS requirements. Flap must be coated with a suitable remoistenable glue that will securely seal the envelope without adhering to contents, not permit resealing of the envelope, and permit easy opening by the recipient.

BEVE Mail-Out Envelope (4-1/8 x 9-1/2"): Envelope must be open side, with gummed, fold-over flap for sealing and contain high-cut diagonal seams or double side seams, at contractor's option. Flap depth must meet USPS standards and flap must be coated with a suitable remoistenable glue that will securely seal the envelope without adhering to contents, not permit resealing of the envelope, and permit easy opening by the recipient.

Face of envelope to contain one die-cut address window (4-1/4 x 1-3/4" in size) with slightly rounded corners. Die-cut window is to be located 1/2" from the bottom edge of the envelope and 3/4" from the left edge of the envelope (the long dimension of the window is to be parallel to the long dimension of the envelope). 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 barcode on the notice is not obscured, and other extraneous information is not visible when material is inserted into the envelope.

Window is to be covered with a suitable, low-gloss, transparent 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 U.S. Postal Service's readability standards/requirements.

eRPA Mail-Out Envelope (6-1/8 x 9-1/2"): Envelope must be open side, with gummed, fold-over flap for sealing and contain high-cut diagonal seams. Flap depth must meet USPS standards and flap must be coated with a suitable remoistenable glue that will securely seal the envelope without adhering to contents, not permit resealing of the envelope, and permit easy opening by the recipient.

Face of envelope to contain one die-cut address window (4-1/4 x 1-1/2" in size) with slightly rounded corners. Die-cut window is to be located 2" from the bottom edge of the envelope and 3/4" from the left edge of the envelope (the long dimension of the window is to be parallel to the long dimension of the envelope). 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 barcode on the notice is not obscured, and other extraneous information is not visible when material is inserted into the envelope.

Window is to be covered with a suitable, low-gloss, transparent 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 U.S. Postal Service's readability standards/requirements.

INSERTING AND PACKING: Gather all pages of a notice in numerical sequence. Notice leaves are to be nested together with all faces forward. Fold from a flat size of 8-1/2 x 11" down to 8-1/2 x 3-11/16" or 8-1/2 x 5-1/2", as indicated, title out.

The address on first page of notice must be visible through window of mail-out envelope. Either wraparound or accordion folds will be acceptable for the trifold notices.

NOTE: Bilingual Spanish/English notices consist of two parts: the first part is a Spanish notice; the second part is the same notice in English. The two parts must be nested together.

Gather folded notice leaves and insert into appropriate mail-out envelope with the recipient's name and address on the first page facing out for visibility through envelope window.

When required, the return envelope is to be inserted behind the notice (when viewed from the window side of the envelope). For the eRPA bilingual notices, the Spanish notice must be in front of the corresponding English notice prior to folding and inserting.

It is the contractor's responsibility to assure that only the computer-generated address and Intelligent Mail Barcode on the notice will be visible through the window in the envelope and that only one notice, and if required, only one of the required return envelope(s) is inserted into each envelope.

Seal envelopes.

Delivered Shipments – Pack suitable in shipping containers.

Mailed Shipments – Mail each individual mailer.

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/imaging of notices, collating, folding, inserting, 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.

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

NOTE: Before production begins on any new workloads, a production inspection may be required at the contractor's plant.

DISTRIBUTION:

- Deliver f.o.b. destination (on the first order and any order that requires a significant change to the language, format, or appearance of a notice) 30 complete sample mailers of each notice type (along with any required insert(s)) inserted into mailout envelopes. DO NOT SEAL ENVELOPES. Deliver samples to: SSA, Printing Management Branch (see Exhibit K).

- Deliver f.o.b. destination one (1) copy of the above specified sample to: Social Security Administration, Wilkes-Barre Direct Operations Center (see Exhibit K).

- Deliver f.o.b. destination on the first order and any order that requires a copy change, 10 samples of each envelope type to: SSA, Mail and Postage Policy Team (see Exhibit K).

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

All mailing shall be made at the First Class rate.

The contractor must use SSA's "Postage and Fees Paid First Class Mail" mailing permit. The mailing permit must be printed on each mail piece.

SSA requires the use of a Permit Imprint. Orders may contain various weight pieces. 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 indicia showing that postage is paid.

Permit imprint indicia may be printed directly onto mail pieces. Permit imprint mailings must contain at least 200 pieces or 50 pounds. The contractor is cautioned to use the permit imprint only for mailing material produced under this contract.

The contractor is strongly encouraged to use manifest mail when postal regulations allow. The contractor must have a Manifest Mailing System (MMS) for First-Class Mail, which has been approved by USPS to document postage charges for this mailing. Each mail piece must be identified with a unique identification number or with a keyline containing a unique identification number and rate information about the piece. Contractor must be in accordance with the MMS in effect at the time of mailing. The requirements for the MMS are contained in Publication 401 "USPS Guide to the Manifest Mailing System." A copy of the USPS approval for the MMS must be presented at the postaward conference**.**

Workload orders that result in mailings of less than 200 pieces or less than 50 pounds will require the contractor to apply the appropriate postage to each piece or meter, at contractor's option. When postage is applied to the mail piece, the permit imprint indicia must be covered/concealed by a meter strip. The contractor will be reimbursed for postage by submitting a properly completed U.S. Postal Service form (or equivalent) with their billing invoice.

Permit imprint may not be used if the mailing is less than 200 pieces. Instead, the mail must be metered and any permit imprint must be covered/concealed by a meter strip. The contractor will be reimbursed for the metered postage by submitting a properly completed Postal Service form (or equivalent).

NOTE*: All meter equipment and supplies must be borne by the contractor.*

Certificate of Conformance: When using Permit Imprint Mail the contractor must complete GPO Form 712 - Certificate of Conformance (Rev. 10-15), and the appropriate mailing statement or statements supplied by USPS. 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.

There is an exception in the Domestic Mail Manual (DMM) called the Minimum Volume Reduction. Contractors are strongly encouraged to apply for the Minimum Volume Reduction through their local BMU and USPS Headquarters in Washington, DC. With the Minimum Volume Reduction exception, contractors will be allowed to mail pieces under 200 pieces, less than 50 pounds on a permit imprint eliminating metering.

If a Government meter is required: The contractor is responsible for the security of the SSA postage meters and access is to be restricted to authorized personnel only. Contractors are to place SSA postage meters in a locked position and place them in a secure server room or safe when not in use. The contractor is to advise all staff there is a penalty for the private use of official postage meters (39USC3203).

Contractors should always maintain sufficient postage on the SSA meters. The contractor should contact SSA if they are not sure of how much postage to load or frequency.

The contractor is required to submit spoiled postage/postage error envelope(s)/meter strip(s) and prepare a Postal Service Form 3533, Application for Refund of Fees, Products and Withdraw of Customer Accounts.

Forms are not obtainable from the United States Postal Service website since they contain a barcode making each form unique. Contractors must go to local Post Offices, postal retail units, or Bulk Mailing Units to obtain the hard copy version of the revised PS Form 3533. USPS will credit the postage refund to SSA through the Official Mail Accounting System (OMAS). SSA requires the contractor to submit a copy of Form 3533 along with the associated print order in which the spoilage occurred and all other postal documentation to the SSA COTR.

The contractor must have approval from SSA's Postage Meter Accountability Team for turn-in of SSA postage meter(s) to the meter manufacturer (e.g., excess meter, defective meter, etc.). If the contractor requires a replacement postage meter, USPS credits any remaining postage to SSA through the USPS' Official Mail Accounting System (OMAS), or the meter manufacturer may transfer the remaining postage from the old meter to the new meter. The contractor is to document the last meter reading (postage remaining amount) before the meter is checked out of service. The contractor may receive a PS Form 3601-C, Postage Meter Activity Report from the meter manufacturer. The contractor is to forward a copy of this report to SSA within **three (3) workdays** of the transaction.

On the first workday of each month, the contractor must load $5.00 on all SSA postage meters (including backup postage meters). In addition to the monthly upload, the Government reserves the right to request the contractor to upload additional funds at any time. These uploads are in addition to any routine meter replenishments. As a result of the postage uploads, the contractor may receive a Postage Meter Reset Activity Report Statement from the meter manufacturer. If received, the contractor should retain this documentation for 12 months.

Contractor is not to relocate SSA postage meters to any other building. Contactors are required to contact the SSA COTR before any movement of an SSA postage meter.

The contractor is required to prepare all metered mail in accordance with the rules and regulations in USPS's Domestic Mail Manual and International Mail Manual**.**

NOTE: Contractors should not receive invoicing for meter rentals. If the contractor receives an invoice, they are to contact the SSA COTR immediately.

Contractor Sites Using "Official Government" Postage Meters with Automated Reporting Capability (Detailed and Limited): Postage meters with "Detailed Account Reporting" are capable of providing trend reports, postal class reports, summary reports, chart production, accounts, subaccounts, operator IDs, etc. These meters provide SSA with remote tracking per print program of postage used. This is SSA's preferred meter type. This meter type is ideal for use when processing multiple SSA workloads because of the account and subaccount feature. Contractors will be required to utilize the postage meter account feature for each SSA print program. Contractors may also be required to use subaccount features for each SSA program. If a contractor requires assistance with setup and operating the "accounting" features of the postage meters, SSA will provide a contact to assist them.

Postage meters with "Limited Account Reporting" are capable of providing SSA with remote tracking of the meter date, contractor/location, meter used, start funds available, any refills/refunds, number of pieces (postage applied), total cost, end funds available, and postage used. This meter is best suited for use when processing one single SSA workload. No action is necessary on the part of the contractor since SSA will be viewing postage meter usage remotely for the individual workload.

Contractor Sites Using an SSA Postage Meter Activity Log (Manual Process): Contractors using mailing equipment that cannot support a postage meter with an internal accounting feature and/or capable of remotely providing SSA with the detailed data it requires when producing multiple workloads will receive a compatible meter but will be required to complete an SSA Postage Meter Activity Log (**Exhibit P**).

The contractor will forward a completed SSA Postage Meter Activity Log to the appropriate SSA COTR or backup for each print order. If the contractor is producing multiple workloads using the same postage meter, the contractor is required to send the log to each SSA COTR/backup. Every field must contain an entry or an "N/A" if the field does not apply. SSA will return incomplete or incorrect activity logs to the contractor for correction. If a primary meter fails and a backup meter is needed to complete the workload, the contractor will need to document the primary meter log in the note field (i.e., meter failed, out of postage, etc.) and create a new activity log (documenting the necessary fields) to use with the backup meter.

Use of the above accounting feature or manual logs does not alter the current postal process. Contractors will continue to forward all postal documentation as required in the contract requirements.

Domestic First-Class Letter-Size Mail: The contractor is required to prepare domestic First Class letter-size mail and obtain the maximum postage discount allowed by the USPS 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.

The contractor is required to prepare Domestic First Class letter-size mail pieces and obtain the maximum postage discount allowed by USPS in accordance with the appropriate USPS rules and regulations, including USPS Domestic Mail Manual and Postal Bulletins on Automation-Compatible First-Class Domestic Mail-Automated and Non-automated mail discount structure in effect at the time of the mailing: a) Automation (5-digit); (b) Automation (3-digit); (c) Automation (AADC); (d) Automation (Mixed AADC); (e) Nonautomation (Presorted); and (f) Nonautomation (Single Piece).

Contractor will be required to produce and use a USPS Intelligent Mail Barcode (IMB) with 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 notices/mail pieces of this workload. The contractor is required to be capable of achieving the postage discounts available with the Full-Service option of the IMB program.

To achieve the maximum automation compatible postal discount, the contractor is required to either presort the notices prior to printing or sort the mail after the notices are inserted. The contractor may use a presort subcontractor for the mailing portion of the contract. SSA has the right to inspect the subcontractor for the security of the mailing operation and compliance with the contract. All of the pieces without a barcode must be separated and mailed as a non-automation rate single piece mailing.

NOTE: Mail addressed to United States territories and possessions (American Samoa, Federated States of Micronesia, Guam, Marshall Islands, Northern Mariana Islands, Palau, Puerto Rico, Virgin Islands, Wake Island, and Military Overseas Addresses (APO/FPO mail) is Domestic Mail, not International Mail.

Intelligent Mail 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.

The 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" between the left and right edges of the window, and at least 0.028" clearance between the Intelligent Mail Bar code 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 ordering 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.

Contractor should be aware that USPS uses the Mail Evaluation Readability Look-up Instrument (MERLIN) to evaluate barcodes. If MERLIN is in effect in the contractor's geographic area, the contractor must ensure that all barcoded mail meets the new barcode standards. The contractor will be responsible for payment of any additional postage resulting from a loss of such discounts due to failure of the contractor-generated barcodes to pass the MERLIN test because of inaccuracy or failure to conform to USPS specifications.

The contractor is responsible for producing and providing all reporting data required for acceptance and processing of full- service mail required by USPS for the Intelligent Mail barcode.

International First-Class Mail: All items mailed must conform to the appropriate USPS International Mail Manual (IMM), Postal Bulletins, and other USPS rules and regulations in effect at the time of mailing.

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 for IPA at the time of the mailing. To maximize postage savings, the contractor will sort to the IPA Rate Group 1 through 15 levels.

Pieces not qualifying for the IPA Rate Group Levels of discount will be prepared at the Worldwide Non-presorted rate level and any remaining pieces that do not meet the IPA qualifications will be sorted by individual country rules according to the USPS IMM in effect at the time of the mailing.

International Mail return addresses must show as the last line of the address "UNITED STATES OF AMERICA" or "USA" in all capital 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 this requirement.

NOTE: International mail cannot contain a presort endorsement.

The contractor is cautioned that files listed will contain mail addressed to United States territories and possessions (American Samoa, Federated States of Micronesia, Guam, Marshall Islands, Northern Mariana Islands, Palau, Puerto Rico, Virgin Islands, Wake Island, and Military Overseas Addresses (APO/FPO mail). This mail is considered Domestic Mail, NOT International Mail and must be included in the discount sorting above.

National Change of Address (NCOA) and Coding Accuracy Support System (CASS): 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.

Contractor cannot at any time change the SSA supplied address prior to receipt by the USPS.

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. Contractor will be required to provide USPS postal discounts for the balance of mail pieces that pass NCOA.

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 GPO's Form 712 (Certificate of Conformance), 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.

NOTE: The contractor will use the Federal Agency Cost Code of 276-00012 on all postal mailing documents.

Within 72 hours of completion of each print order, the contractor must provide PDF copies of the mailing documentation, USPS 3607R, GPO Form 712, and 100% Accountability Summary reports to SSA, Printing Management Branch (see Exhibit K) via email. All copies must be legible and include both obverse and reverse side.

The contractor will be required to forward photocopies of Postal Form 3533 (to USPS for credit), Postage Meter Activity Report forms, and all postage meter replenishment receipts (from the meter vendor) to SSA, Mail and Postage Policy Team (see Exhibit K). Furnished material and USPS validated copies of postal documentation must be delivered (via overnight carrier) to the SSA, Printing Management Branch (see Exhibit K).

Upon completion of this contract, the contractor must return all furnished materials (as applicable) to: Social Security Administration, Attn: SSA, Cheryl Tarver, 3-B-9-D Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401

All expenses incidental to picking up and returning materials (as applicable), submitting proofs, 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 individual electronic task order or print order (GPO form 2511), as applicable.

When required, furnished material must be picked up from and returned to: Social Security Administration, Printing Management Branch (see Exhibit K).

Contractor to email PDF soft proofs to: cheryl.tarver@ssa.gov. (Email must include program and print order numbers plus return name and email address.)

The first task order for live production will be issued on December 1, 2021.

Proof Schedule:

The following schedule begins the workday after notification of the availability of the print order and furnished material. The workday after notification will be the first workday of the schedule.

- Contractor must submit PDF soft proofs for all envelopes within **seven (7) workdays** of receipt of furnished materials.

- Proofs will be withheld no more than **five (5) workdays** from their receipt at the ordering agency until the ordering agency provides changes/corrections/"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 necessary due to author's alterations, contractor to submit revised proofs within **five (5) workdays** of receipt of ordering agency's changes.

- Revised proofs will be withheld no more than **three (3) workdays** from their receipt at the ordering agency until the ordering agency provides changes/corrections/"O.K. to Print" via email. (**NOTE**: The first workday after receipt of revised proofs at the ordering agency is day one (1) of the hold time.)

Preproduction Test Schedules:

Prior to receiving transmission of live production data files, the contractor will be required to perform the below tests. (The transmission tests will begin after the Government is notified of the availability of the system.)

In order for proper arrangements to be made, notification must be given at least **three (3) workdays** prior to all tests.

NOTE: Failure of the contractor to perform any of the below tests satisfactorily may be cause for default. The Government reserves the right to waive the requirements of these tests. The contractor will be notified at the Postaward Conference if any test(s) will be waived.

Transmission Test:

- This test is to be performed within **one (1) week** of the data connection being installed.

- The contractor will be required to receive within **one (1) workday** approximately 141,292 notices.

- The contractor will be required to perform a record count verification and perform the CASS certifications the same workday as receipt of the complete transmission of the test file and must provide SSA with the exact counts and the CASS certification.

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

- When the record count verification has been successfully completed, the contractor will be required to provide SSA, Printing Management Branch (see **Exhibit K**) within **two (2) workdays**, 30 samples from each mailer from the Transmission Test. (See "PREPRODUCTION TESTS, *Transmission Test*.")

- The Government will approve, conditionally approve, or disapprove the samples from the Transmission Test within **five (5) workdays** of receipt thereof. (See "PREPRODUCTION TESTS, *Transmission Test*.")

Preproduction Validation Test:

- Within **five (5) workdays** of receipt of test files and prior to the Preproduction Press and Mail Run test, the contractor is required to perform a Preproduction Validation Test.

- The contractor must furnish SSA not less than 225 total printed samples, as specified (from the furnished test files).

- The Government will approve, conditionally approve, or disapprove the samples from the Preproduction Validation Test within **five (5) workdays** of receipt thereof. (See "PREPRODUCTION TESTS, *Preproduction Validation Test*.")

eRPA Payment Stub Validation Test:

- Within **five (5) workdays** after receipt of test files and prior to the Preproduction Press and Mail Run Test, the contractor will be required to perform the eRPA Daily Notice Payment Stub Validation Test.

- Contractor to submit 100 printed samples of Form SSA-L732-OP1 containing a payment stub for validation of the scanline.

- The Government will approve, conditionally approve, or disapprove the samples from the Preproduction Validation Test within **five (5) workdays** of receipt thereof. (See "PREPRODUCTION TESTS, *Payment Stub Validation Test (eRPA OP1 only)*.")

Preproduction Press and Mail Run Test (24-Hour Test):

- Within **five (5) workdays** of receipt of test files and after the contractor receives the materials necessary to perform the test, the contractor will be required to perform a 24-hour press and mail run test on their equipment and using their personnel.

  The test will occur during the regular work week of Monday through Friday (excluding Federal holidays).

- The contractor will be required to print and prepare for mailing 56,945 notices in a continuous 24-hour period. The mailers will be produced in accordance with all contract specifications and USPS regulations. (See "PREPRODUCTION TESTS, *Preproduction Press and Mail Run Test (24-Hour Test)*.")

- The Government will approve, conditionally approve, or disapprove the samples within **seven (7) workdays** of receipt thereof.

Systems Change/Signature Change/New Notice Files Validation Test:

- When required, the contractor will furnish 100 printed samples (no envelopes or inserts) within **five (5) workdays** of receipt of test files.

- The Government will approve, conditionally approve, or disapprove the samples within **seven (7) workdays** of receipt thereof.

Production Schedule:

Workday – The term "workday" is defined as Monday through Friday each week, excluding the days on which Federal Government holidays are observed. Also excluded are those days on which the Government Publishing Office is not open for the transaction of business, such days of national mourning, hazardous weather, etc.

Federal Government Holidays are as follows: New Year's Day, Martin Luther King's Birthday, Presidents' Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day, and Christmas Day.

The contractor's FTMS software must 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).

Live production files will be transmitted on a daily basis Monday through Saturday for the BEVE and eRPA notices, except for Federal holidays in which case the data will be transmitted on the next day (i.e., when a Federal holiday falls on a Friday, production files will be transmitted on Saturday).

Contractor must not proceed with processing a transmission until counts are verified against the task order. If a discrepancy is found, the contractor must call SSA's Scheduling Helpline immediately at 410-966-5469.

EAD and YCER: Complete production and mailing must be made within **seven (7) workdays** after receipt of each complete transmission.

BEVE and eRPA: Complete production and mailing must be made within **three (3) workdays** after receipt of each complete transmission (e.g., transmissions received on Monday must be mailed by close of business the following Thursday; transmissions received on Saturday must be mailed by the close of business the following Wednesday).

New Notices (Mailer X): Complete production and mailing must be made on these notices within **three (3) to seven (7) workdays** after receipt of each complete transmission as specified by the Government.

PRESS SHEET AND PRODUCTION INSPECTIONS: The contractor must notify the GPO and SSA of the date and time the press sheet or production inspection can be performed. In order for proper arrangements to be made, notification must be given at least 72 hours 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 SSA (see Exhibit K). Telephone calls 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, notification must be given at least 72 hours 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 destinations specified, and 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, labels, etc. will be furnished with each 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. Personnel receiving email 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 requirements 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 for a like period of time.

The following item designations correspond to those listed in the "SCHEDULE OF PRICES."

NOTE: The estimates below represent 12 months of production. However, due to the preproduction requirements, the first year of the contract (the base term) will have only approximately nine (9) months of live production.

I.		8
II.		9
III.	(a)	1
	(b)	1
	(c)	1
IV.	(a)	250
	(b)	15,076
	(c)	23
	(d)	149
	(e)	50
	(f)	5,352
	(g)	2,186
V.	(a)	15,056
	(b)	23
	(c)	149
	(d)	50
	(e)	5,352
	(f)	2,186
VI.		7,538

SECTION 4 - SCHEDULE OF PRICES

Bids offered are f.o.b. destination for deliveries and f.o.b. contractor's city for all mailing.

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 nonresponsive.

An entry of NC (No Charge) must 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 nonresponsive.

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 V. "PAPER."

I. COMPOSITION: Prices offered must include the cost of all required materials and operations necessary for the complete composition for each of the eight (8) envelopes in accordance with these specifications.

Envelopes.....per envelope.....$_____

II. PROCESSING/FORMATTING FILES: The contractor will be allowed only one (1) charge per mailer for the term of the contract to process and/or format the AFP files, AFP Resources, and the Mail Run Data files supplied necessary to print and mail the package.

Processing/Formatting Files.....per mailer.....$_____

_____
(Initials)

III. PREPRODUCTION TESTS: Price offered must include all costs incurred in performing the Transmission Test, Preproduction Validation Test, and Payment Stub Validation Test (for eRPA OP1 only), as specified in these specifications. These costs shall cover but are not limited to: machine time, personnel, all required materials, transmissions, electronic prepress, paper, printing, imaging, collating, inserting, mail preparation, and any other operations necessary to produce the required quantities of the product in the time specified and in accordance with specifications.

(a) Transmission Test..... per test.....$_____

(b) Preproduction Validation Tests ..... per test.....$_____

(c) Payment Stub Validation Test (eRPA OP1 only)..... per test.....$_____

IV. PRINTING/IMAGING, BINDING, AND CONSTRUCTION: Prices offered must be all-inclusive and include the cost of all materials and operations (including proofs, excluding paper) necessary for the printing/imaging, binding, and construction of the product listed in accordance with these specifications.

NOTE: Prices must include the cost of packing and distribution of deliveries only.

(a) *Daily Makeready/Setup Charge .....$_____

*Contractor will be allowed only one (1) makeready/setup charge per workday (maximum 5 per print order). This combined charge shall include all materials and operations necessary to makeready and/or setup the contractor's equipment for all mailers run each day. Invoices submitted with more than one makeready/setup charge per workday will be disallowed.

(b) Notice Leaves ..... per 1,000 leaves.....$_____

(c) White CRM Envelope (5-3/4 x 8-3/4") ..... per 1,000 envelopes.....$_____

(d) White BRM Envelope (5-3/4 x 8-3/4") ..... per 1,000 envelopes.....$_____

(e) Green BRM Envelope (3-7/8 x 8-7/8") ..... per 1,000 envelopes.....$_____

(f) Mail-Out Envelope (4-1/8 x 9-1/2")..... per 1,000 envelopes.....$_____

(g) Mail-Out Envelope (6-1/8 x 9-1/2")..... per 1,000 envelopes.....$_____

V. PAPER: Payment for all paper supplied by the contractor under the terms of these specifications, as ordered on the individual task order/print order, 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:

Personalized Notices: A charge will be allowed for each page-size leaf.
All Envelopes: One leaf will be allowed for each envelope.

_____
(Initials)

Per 1,000 Leaves

(a) Personalized Notices: White OCR Bond (20-lb.).....$_____

(b) White CRM Envelope (5-3/4 x 8-3/4"): White Writing Envelope (20-lb.).....$_____

(c) White BRM Envelope (5-3/4 x 8-3/4"): White Writing Envelope (20-lb.).....$_____

(d) Green BRM Envelope (3-7/8 x 8-7/8"): Green Writing Envelope (20-lb.).....$_____

(e) Mail-Out Envelope (4-1/8 x 9-1/2"): White Writing Envelope (24-lb.);
or at contractor's option, White Uncoated Text (60-lb.) .....$_____

(f) Mail-Out Envelope (6-1/8 x 9-1/2"): White Writing Envelope (24-lb.);
or at contractor's option, White Uncoated Text (60-lb.) .....$_____

VI. INSERTING 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 collating notice(s) (single or multiple leaves) in proper sequence; folding to required size in accordance with these specifications; insertion of notice(s) and appropriate reply envelope (if required) into appropriate mail-out envelope; and, mailing in accordance with these specifications.

Mailers ..... per 1,000 mailers .....$_____

LOCATION OF POST OFFICE: All mailing will be made from the_____

Post Office located at Street Address _____,

City_____, State _____, Zip Code _____

_____
(Initials)

SHIPMENT(S): 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 Solicitation 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 (60 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 points(s), in exact accordance with specifications. ***NOTE****: Failure to provide a 60-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 certifications 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 Name) (GPO Contractor's Code)

_____
(Street Address)

_____
(City – State – Zip Code)

By _____
(Printed Name, Signature, and Title of Person Authorized to Sign this Bid) (Date)

_____
(Person to be Contacted) (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 civil or criminal prosecution under Federal law.

----------	----------
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

EXHIBIT B

SSA External Service Provider Additional Security Requirements

All External Service Providers (ESP) are subject to the following security requirements:

- All ESPs are subjected to SSA's Security Authorization Process, which will entail security testing and evaluation of the in-place security controls. For more information, see NIST SP 800-37, Revision 2 - Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy, December 2018.
- ESPs must follow NIST SP 800-53 Revision 4 *Recommended Security Controls for Federal Information Systems and Organizations* for protecting Low or Moderate impact level information as categorized by FIPS 199 for the information system. Note: Systems that contain Personally Identifiable Information (PII) are considered "Moderate".
- ESPs must document all deployed (applicable) and planned controls for an information system in a System Security Plan that is in NIST-compliant format. SSA will provide the SSP template to be completed.
- ESPs classified as Cloud Service Providers (CSP) must adhere to additional FedRAMP security control requirements. Further information may be found at: **http://www.gsa.gov/portal/category/102371.** As part of these requirements, CSPs must have a security control assessment performed by a Third Party Assessment Organization (3PAO).
- Upon request from SSA, the ESP shall provide the following network security information and documentation for review and audit purposes:
    - All information security control artifacts required to support the Security Assessment and Authorization (SA&A) process.
    - Intrusion Detection Systems (IDS) configuration.
    - Network firewall configuration.
    - Server and network device patching schedules and compliance.
    - Server, network device, and security logs.
    - Detailed hardware inventory including servers, network devices, and storage.

ESPs are required to adhere to NIST 800-53 Rev 4 security control framework based on their assigned categorization. The following sections outline additional security controls and SSA organizational defined parameters for NIST 800-53, Rev 4. Security requirements below are applicable to low and moderately categorized systems unless otherwise designated. For additional information or supplement guidance for these controls, refer to Appendix F - SECURITY CONTROL CATALOG in NIST 800-53, Rev 4.

Account Management Requirements

The purpose of the following is to address requirements for **account and session management** for External Service Providers (ESPs).

SSA Additional Requirements for ESPs:

- **AC-2** - ESPs must employ individual account types on external service provider systems. The use of group, anonymous or temporary accounts is strictly prohibited.
- **AC-2** - ESPs must demonstrate the implementation of an approval process that describes how system accounts are created, deleted, disabled, or modified. The process should account for roles in the system and the appropriate authorizations to grant access. Public-facing systems may use a registration process in place of the approval process.
- **AC-2(3)** - A deactivation process is required to manage inactive accounts. The process must describe how the system identifies and deactivates inactive accounts that have not been in use for 90 days or more. ESPs must *automatically* disable inactive accounts after 90 days and then remove these disabled accounts after 1 year.
- **AC-2(4)** - ESPs must provide the capability to produce a record of all account management activities that occur on the system and develop an automated method to submit these records in the form of a report to SSA.
- **AC-6** - ESP administrator accounts and privileged user accounts must be customized to only allow access to specific roles and functions on the system. ESP must provide a list of these functions to the Contract Officer Technical Representative (COTR). (Moderate and High categorized systems only).
- **AC-7** - ESPs must enforce a limit of 3 consecutive invalid login attempts by a user during a 20-minute period and automatically lock the account/node for 30 minutes when the maximum number of unsuccessful attempts is exceeded. The account shall remain locked for 30 minutes. (Moderate and High categorized systems only).
- **AC-8** - ESPs providing services to SSA internal users must display the internally used and approved warning banner.
  - The SSA internal banner is as follows:
    - Only authorized users can access the system.
    - The system is a U.S. Government computer system subject to Federal law.
    - Unauthorized attempts to access or modify any part of SSA's systems are prohibited and subject to disciplinary, civil action or criminal prosecution.

  If the system is serving the public as its user base, the system must display a warning banner containing language that is appropriate to the application. The SSA COTR must approve the public warning banner language prior to implementation.
- **AC-11** - ESPs must enforce termination of user sessions after 30 minutes of inactivity. Users must authenticate again after sessions are terminated in order to continue using the application. (Moderate and High categorized systems only).
- **AC-17(4)** - ESPs must restrict remote access to approved administrative functions and accounts.

Awareness and Training Requirements

The purpose of the following is to address requirements for **awareness and training** for External Service Providers (ESPs).

SSA Additional Requirements for ESPs:

- **AT-2 -** ESP contractors and their employees or sub-contractors must complete SSA provided security awareness training at least annually.
- **AT-3 -** ESPs must provide role-based training to all employees who fulfill special roles or duties in regards to SSA data or systems.
- **AT-4** - ESPs must retain and produce records of role based training completions for 3 years.

Auditing Requirements

The purpose of the following is to address requirements for **auditing** for External Service Providers (ESPs).

SSA Additional Requirements for ESPs:

- **AU-2** - ESPs must maintain an audit log of transactions create, modify, or delete SSA information.
- **AU-2** - ESPs must maintain an audit log of the following events: Logon/logoff events, account management, privilege or role changes, and administrator activity.
- **AU-5 -** ESPs must report any failure of audit processing that occurs to the SSA COTR within 24 hours.
- **AU-6 -** ESPs must review and analyze information system audit record for indications of inappropriate or unusual activity and report those findings to SSA COTR within 24 hours. ESPs must support monitoring and review of the system for unusual or inappropriate activity daily. This activity must be provided to the COTR immediately for review.
- **AU-6 -** ESPs must provide user and transaction log reports to SSA when requested**.**
- **AU-7(1) -** ESPs must allow for scoping of audit criteria for efficient reporting capability.
- **AU-11 -** ESPs must retain online audit logs for 90 days.
- **AU-11 -** ESPs must retain audit records for seven (7) years.

Security Assessments and Authorization Requirements

The purpose of the following is to address requirements for **security assessments and authorization** for External Service Providers (ESPs).

SSA Additional Requirements for ESPs:

- **CA-2 -** ESPs must develop an assessment plan that includes:
    - Annual assessment of a subset of controls

- Triennial comprehensive assessment (full scope)
- Assessments as needed when a significant change occurs on the system.

- **CA-2 -** ESP and COTR must define what a significant change is and require a new assessment whenever a significant change occurs. *Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.*
- **CA-3 -** The contractor shall document in the SSA security plan, all connections to contractor resources made to external information systems, and applications. Examples of connections would include: connections to subcontractor sites, connections used for remote administration, connections made to contractor's company/corporate networks, etc. These connections shall be reviewed and monitored on an ongoing basis, at least annually to determine the need for ongoing use by the contractor management. (Moderately categorized systems only).
- **CA-5 -** For any security reports issued to the contractor, including internal independent reviews, the contractor is responsible for developing a POA&M that identifies corrective actions and/or mitigating controls for any identified vulnerabilities. Contractors shall report to COTR POA&M progress at least monthly. In addition, the contractor must provide artifacts to update POA&M items at least 7 days prior to milestone completion date to ensure SSA has sufficient time to review.
- **CA-7** - ESP must monitoring the effectiveness of its security controls on a continual basis and take appropriate corrective actions as necessary to ensure SSA data is protected from unauthorized access, modification or disclosure.

Configuration Management Requirements

The purpose of the following is to address requirements for **configuration management** for External Service Providers.

SSA Additional Requirements for ESPs:

- **CM-2(3) -** ESPs must define and deploy an approved device configuration on each device used to provide services to SSA at least annually.
- **CM-6** - ESPs must periodically scan the device configuration of each device used to provide services to SSA and identify deviations from the approved device configuration. Deviations shall be logged and corrected within 24 hours. The ESP shall submit device scan reports to SSA upon request.
- **CM-8** - ESPs must maintain an inventory all IT assets that store, process, or transmit SSA data and provide to SSA upon request.
- **CM-9 -** The contractor shall maintain a configuration management plan that addresses the roles, responsibilities, processes, and procedures to manage inventory throughout the lifecycle.

Contingency Planning Requirements

The purpose of the following is to address requirements for **contingency planning** for External Service Providers.

SSA Additional Requirements for ESPs:

- **CP-2 -** ESP must submit a contingency plan that will support and meet the SSA supplied recovery objectives and must be maintained, reviewed and, if necessary updated at least annually.
- **CP-9 -** ESPs must encrypt all Media used for backup and archiving purposes using Federal Information Processing Standard (FIPS) 140-2 compliant solutions. (Moderate and High categorized systems only).

Identification and Authentication Requirements

The purpose of the following is to address requirements for **identification and authentication** for External Service Providers (ESPs).

SSA Additional Requirements for ESPs:

- **IA-2(12)** - Identity, Authorization and Access Management (IdAAM) - The External Service Providers must seamlessly integrate with the SSA's Federation Service. This service is based on oAuth and SAML (Security Assertion Markup Language) 2.0 standards and enables SSA to meet its two factor authentication requirements as specified in Homeland Security Presidential Directive (HSPD)-12, dated August 12, 2004. This service enables SSA to leverage an internal Microsoft's Active Directory to create a single SSA-Wide directory of all users. Currently, SSA users are required to authenticate using their SSA HSPD-12 PIV Smart Card at the workstation. In certain acceptable instances, users can revert to user name and password, while the Department is transitioning to HSPD-12 PIV Smart Card Authentication. The External Service Providers must support both authentications methods.
- **IA-6 -** ESPs must mask all fields on a system that has a logon screen that requires credentials, to prevent unauthorized exposure.
- **IA-7 -** The ESP must encrypt credentials used for e-authentication. The encryption solution must be compliant with FIPS 140-2. (Moderate and High categorized systems only).

Incident Response Requirements

The purpose of the following is to address requirements for **incident response** for External Service Providers.

SSA Additional Requirements for ESPs:

- **IR-6 -** ESPs will receive the incident response capability timeframe and reporting requirements from the SSA COTR.
- **IR-6 -** ESPs Incident Response plan must require all security incidents of US CERT categories 1,2,3,4 and 6 must be reported to SSA COTR.
- **IR-7 -** ESPs are responsible for notifying the appropriate SSA COTR when there is a security incident that has been categorized 1,2,3,4 or 6 per US CERT regulations. The COTR is authorized to issue orders to take down external systems or components to perform IR, forensics, further loss of data, etc.

Maintenance Requirements

The purpose of the following is to address requirements for **maintenance** for External Service Providers.

SSA Additional Requirements for ESPs:

- **MA-2 -** ESP must retain records of maintenance activities performed on IT devices used to provide services to SSA. Maintenance activity logs must be made available upon request.
- **MA-2 -** IT equipment and media used to provide services to SSA must be sanitized prior to removal from the ESP's facility for maintenance or disposal purposes. The ESP must maintain a log as evidence that the IT equipment or media was sanitized prior to removal. Logs must be made available upon request. Refer to NIST SP 800-88 for more information on media sanitization.

Media Protection Requirements

The purpose of the following is to address requirements for **media protection** for External Service Providers.

SSA Additional Requirements for ESPs:

- **MP-2 -** Removable media used to store SSA data must be encrypted using a FIPS 140-2 compliant encryption solution.
- **MP-3** - ESP must label or mark (human readable) all media containing PII or other sensitive SSA data as "SSA Confidential Unclassified Information". (Moderate and High categorized systems only).
- **MP-4 -** ESP must have a documented process describing how IT equipment and media are controlled to ensure the security and confidentiality of SSA data.
- **MP-5 -** ESP must maintain chain of custody for IT equipment and media during transport outside of controlled-access facilities. Authorized personnel must perform transport of media outside of controlled areas.

Planning Requirements

The purpose of the following is to address requirements for the **planning** for External Service Providers (ESPs).

SSA Additional Requirements for ESPs:

- **PL-2 -** ESP must develop a System Security Plan (SSP) compliant with NIST SP 800-18. The SSP shall be submitted to the SSA COTR.
- **PL-2 -** ESP must conduct an annual security review of the solution used to provide services to SSA. The System Security Plan (SSP) must be updated to reflect changes affecting the security of SSA data.
- **PL-4 -** The SSA COTR will provide the SSA Rules of Behavior (within the SSA Information System Security Handbook) for ESP systems that support internal users providing services to SSA. The rules of behavior ensure users are familiar with information security, privacy, and confidentiality practices.

Personnel Security Requirements

The purpose of the following is to address requirements for **personnel security** for External Service Providers.

SSA Additional Requirements for ESPs:

- **PS-4 -** ESP must terminate employee and sub-contractor access to the solution used to provide services to SSA immediately upon reassignment or separation.
- **PS-6 -** ESP personnel who are granted access to IT equipment, media or data used to provide services to SSA must agree and sign a non-disclosure agreement prohibiting unauthorized disclosure of SSA data encountered in the performance of their duties.
- **PS-7 -** ESP sub-contractors are bound to the same security requirements as employees.
- **PS-8** - ESP must inform the SSA project officer of any violation of security requirements within 24 hours.

Risk Assessment Requirements

The purpose of the following is to address requirements for **risk assessment** for External Service Providers (ESPs).

SSA Additional Requirements for ESPs:

- **RA-3 -** ESPs shall conduct a risk assessment to assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of sensitive SSA information. The risk assessment should be reviewed annually and updated every three years or when a significant change occurs.
- **RA-5 -** ESP must scan IT equipment used to provide services to SSA for security vulnerabilities at least monthly. The contractor must use a commercially available scanning tool. The scanning must include vulnerabilities identified in DHS national vulnerability database. Vulnerability scan reports must be retained for 12 months and submitted to the SSA COTR upon request.

System and Communication Requirements

The purpose of the following is to address requirements for **system and communications** for External Service Providers (ESPs).

SSA Additional Requirements for ESPs:

- **SC-4 -** ESP must logically or physically segregate SSA data from that of other customer if a multi-tenant environment is used to provide services to SSA. (Moderate and High categorized systems only).
- **SC-7(1) -** ESPs shall physically allocate publicly accessible information system components to separate subnetworks with separate physical network interfaces.
- **SC-7(4) -** ESPs must provide traffic flow policy for each managed interface to SSA COTR for review and approval prior to implementation.
- **SC-8 -** ESP must encrypt PII and other sensitive SSA data when stored on persistent storage devices, or when transmitted over approved system interconnections, using a FIPS 140-2 compliant encryption solution (Moderate and High categorized systems only).
- **SC-10 -** ESPs must terminate user sessions automatically after 15 minutes of inactivity. (Moderate and High categorized systems only).
- **SC-15 -** ESPs use of collaborative computing devices (e.g., networked whiteboards, cameras, and microphones) on systems hosting /processing/ shall have their remote activation capability removed/disabled.

- **SC-17 -** For all ESPs, who manage information systems, the information system shall utilize automated mechanisms with supporting procedures in place for digital certificate generation, installation, and distribution. Subscriber key pairs are generated and stored using FIPS 140-2 Security Level 2 or higher cryptographic modules. The same public/private key pair is not to be used for both encryption and digital signature. Private keys are protected using, at a minimum, a strong password. A certificate is revoked if the associated private key is compromised; management requests revocation; or the certificate is no longer needed. (Moderate and High categorized systems only).
- **SC-18 -** Mobile code is software that is executed from a host machine to run scripts on a client machine, including animation scripts, movies, etc. Mobile code is a powerful computing tool that can introduce risks to the user's information system. Whenever an ESP is developing or deploying the mobile code technology, this shall be identified in the ESP's security plan to SSA. Contractors, who use mobile code, shall be subject to a source code review by SSA personnel to ensure that there is no potential risk in introducing malicious code into the contractor/user's environment. (Moderate and High categorized systems only).

System and Information Integrity Requirements

The purpose of the following is to address requirements for **system and information integrity** for External Service Providers.

SSA Additional Requirements for ESPs:

- **S1-2 -** ESPs will remediate discovered flaws in the information system according to a process that is approved by the COTR.
- **SI-3 -** ESP must submit alerts on malicious code detection and actions performed on malicious code to the SSA COTR for review.
- **SI-4 -** The ESP shall employ tools and techniques to monitor events on the information system to detect attacks, vulnerabilities, and detect, deter, and report on unauthorized use of the information system. Whenever there is an elevated security level, the monitoring efforts shall be increased as necessary to enable deterrence, detection, and reporting to take place so that corrective actions shall be made to the networked environment.
- **SI-5 -** ESPs must receive advisories (from US CERT) on a regular basis and take appropriate actions as necessary.
- **SI-11 -** The information system shall identify security relevant error conditions and handle error conditions in an expeditious manner. (Moderate and High categorized systems only).

EXHIBIT C

Security Assessment Report

Social Security Administration (SSA)

<System Name> (<Acronym>)

Security Categorization: <Enter Categorization>

<DRAFT/FINAL> Version <x.x>

<Month DD, YYYY>

Prepared by

VERIS GROUP

8229 Boone Blvd., Suite 750

Vienna, VA 22182

TEMPLATE VERSION (V1.3 FY17) - REMOVE BEFORE PUBLISHING

<INSTRUCTIONS: Orange, bracketed text indicates instructions on how a section should be completed or sample text, which should be replaced with project specific information or removed. Ensure sample text is turned from orange to black where necessary (e.g., headings shall be changed to the standard heading color), and all instructions are removed (including this paragraph). Remove the template ID (e.g., TMP V1.3 FY17) from the footer before publishing. All black text shall remain unchanged.>

Assessment Summary

This document describes the Federal Information Security Modernization Act (FISMA) Security Assessment Report (SAR) for Social Security Administration (SSA). The primary purpose of this document is to deliver the independent security assessment findings for <System Name> (hereafter known as <System Acronym>). These findings will lead to the initiation of corrective actions or for making risk-based decisions. This independent security assessment supports the U.S. Government's mandate that all U.S. Federal information systems comply with FISMA of 2014.

The assessment took place between <MM DD, YYYY> and <MM DD, YYYY>. The independent security assessment followed the approved the Security Assessment Plan (SAP). All deviations from the approved SAP are located in Table 7.

The table below represents the aggregate risk identified from the independent security assessment.

Table 1: Executive Summary of Risks

Risk Category	Total	% of Total Risks
High	<# high risks>	<% of total risks>
Moderate	<# moderate risks>	<% of total risks>
Low	<# low risks>	<% of total risks>
Total Risks	**<Sum of all H, M, L risks>**	**100%**

NOTE: Total is the sum of high, moderate, and low risks with operationally required risks being represented as a subset of this total.

Document Revision History

Version	Date	Description	Author
1.0	<10/02/2015>	Initial release	Coalfire
<1.1>	<10/26/2015>	<Final template updates FY17>	Coalfire
<1.2>	<10/24/2017>	<Template updates for FY17>	Coalfire

Table of Contents

List of Tables

1 Introduction

This SAR document for <System Acronym> is required by the National Institute of Standards and Technology (NIST) 800-53 Revision 4 (Rev 4) document. This SAR contains unbiased and factual security findings by an independent security assessment team. This SAR contains the <System Acronym> system specific security controls tested as per the Security Assessment Plan (SAP) approved by SSA Office of Information Security (OIS), the <System Acronym> Security Authorization Manager (SAM), and the Coalfire (formally Veris Group) Project Manager (PM). The implementation status of these controls identify the residual risk (risk remaining after controls have been implemented). These controls are required per NIST 800-53 Rev. 4 to address known information system vulnerabilities. The results are in support of SSA Security Authorization program goals, efforts, and activities necessary to achieve compliance with FISMA security requirements.

1.1 Applicable Laws and Regulations

- Computer Fraud and Abuse Act [Public Law (PL) 99-474, 18 U.S. Code (USC) 1030]
- E-Authentication Guidance for Federal Agencies [Office of Management and Budget (OMB) M-04-04]
- FISMA of 2014 [PL 113-283]
- Freedom of Information Act (FOIA) As Amended in 2002 [PL 104-232, 5 USC 552]
- Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
- Homeland Security Presidential Directive(HSPD)-7, Critical Infrastructure Identification, Prioritization and Protection [HSPD-7]
- Internal Control Systems [OMB Circular A-123]
- Management of Federal Information Resources [OMB Circular A-130]
- Management's Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/2004]
- Privacy Act of 1974 as amended [5 USC 552a]
- Protection of Sensitive Agency Information [OMB M-06-16]
- Records Management by Federal Agencies [44 USC 31]
- Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]
- Security of Federal Automated Information Systems [OMB Circular A-130, Appendix III]

1.2 Applicable Standards and Guidance

- A NIST Definition of Cloud Computing [NIST SP 800-145]
- Computer Security Incident Handling Guide [NIST SP 800-61, Revision 2]
- Contingency Planning Guide for Federal Information Systems [NIST SP 800-34, Revision 1]
- Engineering Principles for Information Technology Security (A Baseline for Achieving Security) [NIST SP 800-27, Revision A]
- Assessing Security and Privacy Controls in Federal Information Systems and Organizations [NIST SP 800-53A, Revision 4]

- Security and Privacy Controls for Federal Information Systems and Organizations [NIST SP 800-53, Revision 4]
- Guide for Developing Security Plans for Federal Information Systems [NIST SP 800-18, Revision 1]
- Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]
- Guide for Mapping Types of Information and Information Systems to Security Categories [NIST SP 800-60, Revision 1]
- Guide for Security-Focused Configuration Management of Information Systems [NIST SP 800-128]
- Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
- Managing Information Security Risk: Organization, Mission, and Information System View [NIST SP 800-39]
- Minimum Security Requirements for Federal Information and Information Systems [FIPS Publication 200]
- Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS Publication 201-2]
- Recommended Security Controls for Federal Information Systems [NIST SP 800-53, Revision 4]
- Guide for Conducting Risk Assessments [NIST SP 800-30, Revision 1]
- Security Considerations in the System Development Life Cycle [NIST SP 800-64, Revision 2]
- Security Requirements for Cryptographic Modules [Federal Information Processing Standard (FIPS) Publication 140-2]
- Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
- Technical Guide to Information Security Testing and Assessment [NIST SP 800-115]

1.3 Purpose

The purpose of this document is to provide the System Owner (SO) and the SSA Authorization Official (AO) with a detailed level of the residual risk for <System Acronym>. An independent security assessment team conducted a test for each system specific security control implemented by SSA stakeholders. These tests include a combination of interviews, document examinations, and actual technical testing of controls when applicable. These controls each had implementation statements listed in the <System Acronym> System Security Plan (SSP). These statements identified how the controls are in place and the assessment team tested the controls based on that criteria. Additionally, the testing ensures the controls are in are in compliance with the FISMA baseline security control requirements as defined in NIST 800-53 Rev 4. FISMA mandates that all Federal Agencies will comply with the NIST 800-53 Rev. 4 standards. Assessors from the independent security assessment team are members of contracted Coalfire Federal Services (formally Veris Group).

The system specific security controls for this assessment are in section 2.1

2 Scope

2.1 Applicable Security Controls

The applicable security controls as listed in the <System Acronym> SAP are in Table 2 of this <System Acronym> SAR. The security control assessment authorized by OIS and the <System Acronym> SAM gives authority to the Coalfire Independent Security Assessment team to assess the listed controls.

Table 2: Identified Security Controls Assessed

Security Control Family	Security Control
Access Control	AC-2, AC-2(2), AC-2(3), AC-2(4)
Awareness and Training	
Audit and Accountability	AU-7(1)
Security Assessment and Authorization	CA-5, CA-6
Configuration Management	CM-9
Contingency Planning	
Identification and Authentication	IA-2, IA-(3), IA-5, IA-5(1)
Planning	PL-2, PL-2(3), PL-8
Personnel Security	PS-4, PS-5
Risk Assessment	RA-2, RA-3
System and Services Acquisition	SA-3, SA-4(9), SA-5, SA-8, SA-9, SA-9(2), SA-11
System and Communications Protection	SC-4, SC-39
System and Information Integrity	SI-10, SI-11, SI-16

2.2 System Name/Title

The <System Acronym> system unique identifier and system acronyms are in Table 3. Due to the number of applications located within <System Acronym>, <only two of the subsystems> fall within the scope of this assessment. The authority to use a representative sample is located within NIST 800-53 Rev 4 Guide for Assessing the Security Controls in Federal Information Systems and Organizations.

Table 3: Information System Name and Title

Information System Name:	<System Name>
Information System Acronym:	<System Acronym>
Information System Identifier	<System Identifier>
Security Categorization: (High, Moderate, Low)	<Categorization>
PII data: (Yes/No)	<Yes/No>
e-Authentication Application: (Yes/No)	<Yes/No>
Production Data Used In Development/Test Environment (Yes/No)	<Yes/No>

Federal Tax Information (Yes/No)	<Yes/No>

2.3 Assessment Documentation

Documentation used by the independent assessment team to perform the assessment of the <System Acronym> subsystems include the following:

- <System Acronym> System Security Plan (SSP)
- <System Acronym> Security Assessment Plan (SAP)
- Security Operation Division (SOC) Nessus scanner with McAfee, McAfee ePolicy Orchestrator (EPO) instance scan statistic reports
- SSA Information Security Policy (ISP)
- The <System Acronym> Boundary Scope Memo (BSM)
- The <System Acronym> Information System Contingency Plan (ISCP)
- The <System Acronym> Federal Information Processing Standards Publication (FIPS) 199

2.4 Location of Components Tested

The physical locations of all the different functional components supporting the testing of the <System Acronym> information system is in Table 4.

Table 4: Location of Components

System Physical Location and Addresses		
Production Environment Site Name	**Address**	**Description of Components**
<EXAMPLE: National Computer Center (NCC)>	6401 Security Blvd Baltimore, MD 21235	Production Environment (i.e., hardware) (Primary Support)
Development/Test Environment Site Name	**Address**	**Description of Components**
<EXAMPLE: National Support Center (NSC)>	3500 Campus Drive, Suite 106 Urbana, MD 21704	Development and Testing Environment (Integration Testing)
Disaster Recovery Environment Site Name	**Address**	**Description of Components**
<EXAMPLE: Secondary Support Center (SSC)>	3004 Tower Blvd Durham, NC 27707	Production Environment (i.e., hardware) (Secondary/Failover Support)
Contractor Owned Environment Site Name	**Address**	**Description of Components**

2.5 Subsystems, Users and Interfaces

The <System Acronym> system contains the following subsystems, users and interfaces that were tested as part of this assessment. They are contained within the embedded **Error! Reference source not found.**.

<Complete the embedded spreadsheet with system specific information.>

Table 5: Users and Interfaces

T2 Internet - Users and Interfaces.doc

<Embed the applicable system's Users and Interface, EXAMPLE attached.>

2.6 Assessment Inventory

The <System Acronym> hardware and software inventories provided by the SO's are in Table 6.

<Complete the embedded spreadsheet with system specific information.>

Table 6: Hardware and Software Inventory

T2 Internet - HW-SW Inventory.xl

<Embed the applicable system's Hardware and Software Inventory, EXAMPLE attached.>

NOTE: Any changes to the scope of the Authorization Boundary after the Boundary Scope Meeting and finalization of the Boundary Scope Memo (BSM) may impact the overall Independent Verification and Validation (IV&V) schedule.

3 System Overview

3.1 Security Categorization

The FIPS 199 *Security Categorization of a Federal Information and Information System* publication determines the risk impact level of data vulnerability exploitation. The identified impact level sets the security control baseline that needs to be tested. The categorization for <System Acronym> determined by the FIPS 199 publication is a Moderate baseline. The NIST 800-53 Rev 4. <Moderate> baseline of controls are assessed during the security assessment.

3.2 System Description and Purpose

<In the sections below, insert a general description of the information system. Use a description that is consistent with the description found in the SSP. The description must only differ from the description in the SSP if additional information is going to be included that is not available in the SSP or if the description in the SSP is not accurate.>

4 Assessment Methodology

A summary of the assessment methodologies used to conduct the security assessment for the <System Acronym> subsystems are in the following steps:

- Perform tests on the listed controls in the <System Acronym> SAP and record the results
- Identify vulnerabilities related to <System Acronym>
- Identify known threats and determine which threats are associated with the cited vulnerabilities
- Analyze risks based on vulnerabilities and associated threats after mitigating controls are implemented
- Recommend corrective actions for controls that are not satisfied (other than satisfied)
- Document all security assessment results, which include identified unmitigated risks, mitigated risks, and recommend corrective actions.

4.1 Perform Tests

Coalfire Federal Services performed security tests on the <System Acronym> subsystems, which concluded on <MM DD, YYYY>. The results of the tests are documented within the Security Risk Traceability Matrix (SRTM) in Appendix B. The SRTM serves as input to this SAR.

4.1.1 Assessment Deviations

Table 7 contains any deviations from the SAP if applicable. Coalfire Federal Services did not deviate from the testing plan.

Table 7: List of Assessment Deviations

Deviation ID	Deviation Description	Justification

4.2 Identification of Vulnerabilities

Coalfire Federal Services conducts an assessment to identify vulnerabilities for <System Acronym> subsystems. These vulnerabilities should have controls in place to mitigate the risk of exploitation.

A vulnerability is an inherent weakness in an information system that can be exploited by a threat or threat agent, resulting in an undesirable impact on the protection of the confidentiality, integrity, or availability of the system (application and associated data). A vulnerability may be due to a design flaw or error in a configuration that makes the network or a host on the network, susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in multiple areas of the system or facilities, such as in firewalls, application servers, Web servers, operating systems, or fire suppression systems.

Whether or not a vulnerability has the potential to be exploited by a threat depends on a number of variables including (but not limited to):

- The strength of the security controls in place
- The ease at which a human actor could purposefully launch an attack
- The probability of an environmental event or disruption in a given local area

An environmental disruption is usually unique to a geographic location. Depending on the level of the risk exposure, the successful exploitation of a vulnerability can vary from disclosure of information about the host to a complete compromise of the host. Risk exposure to organizational operations can affect the business mission, functions, and/or reputation of the organization.

4.3 Consideration of Threats

A threat is an adversarial force or phenomenon that could affect the availability, integrity, or confidentiality of an information system, its networks, and the facility that houses the hardware and software. A threat agent is an element that provides the delivery mechanism for a threat. An entity that initiates the launch of a threat agent is referred to as a threat actor.

A threat actor might purposefully launch a threat agent (e.g., a terrorist igniting a bomb). A threat actor could also be a trusted employee that acts as an agent by making an unintentional human error (e.g., a trusted employee clicks on a phishing email that downloads malware). Threat agents may also be environmental in nature with no purposeful intent (e.g., a hurricane). Threat agents working alone, or in concert, exploit vulnerabilities to create incidents. FISMA categorizes threats using a threat origination taxonomy of purposeful (P), unintentional (U), or environmental (E) type threats as described in Table 8.

Table 8: Threat Categories and Type Identifiers

Threat Origination Category	Type Identifier
Threats launched purposefully	P
Threats created by unintentional human or machine error	U
Threats caused by environmental agents or disruptions	E

Threat actors for a variety of reasons launch purposeful threats and the reasons may never be fully known. Curiosity, monetary gain, political gain, social activism, revenge or many other driving forces could motivate threat actors. It is possible that some threats could have more than one threat origination category.

Some threat types are more likely to occur than others are. FISMA considers threat types to help determine the likelihood that a vulnerability could be exploited. The threat table shown in

Table 9 describes typical threats to information systems; these threats have been considered for <System Acronym>.

Table 9: Potential Threats

ID	Threat Name	Type Identifier	Description	Typical Impact to Data or System		
				Confidentiality	Integrity	Availability
T-1.	Alteration	U, P, E	Alteration of data, files, or records.		Modification	
T-2.	Audit Compromise	P	An unauthorized user gains access to the audit trail and could cause audit records to be deleted or modified, or prevents future audit records from being recorded, thus masking a security relevant event.		Modification or destruction	Unavailable accurate records
T-3.	Bomb	P	An intentional explosion.		Modification or destruction	Denial of service
T-4.	Communications Failure	U, E	Cut fiber optic lines, trees falling on telephone lines.			Denial of service
T-5.	Compromising Emanations	P	Eavesdropping can occur via electronic media directed against large scale electronic facilities that do not process classified National Security Information.	Disclosure		
T-6.	Cyber Brute Force	P	Unauthorized user could gain access to the information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.	Disclosure	Modification or destruction	Denial of service
T-7.	Data Disclosure Attack	P	An attacker uses techniques that could result in the disclosure of sensitive information by exploiting weaknesses in system design or configuration.	Disclosure		
T-8.	Data Entry Error	U	Human inattention, lack of knowledge, and failure to cross-check system activities could contribute to errors becoming integrated and ingrained in automated systems.		Modification	
T-9.	Denial of Service Attack	P	An adversary uses techniques to attack a single target rendering it unable to respond; could cause denial of service for users of the targeted information systems.			Denial of service

ID	Threat Name	Type Identifier	Description	Typical Impact to Data or System		
				Confidentiality	Integrity	Availability
T-10.	Distributed Denial of Service Attack	P	An adversary uses multiple compromised information systems to attack a single target; could cause denial of service for users of the targeted information systems.			Denial of service
T-11.	Earthquake	E	Seismic activity can damage the information system or its facility. Refer to the following document for earthquake probability maps http://pubs.usgs.gov/of/2008/1128/pdf/OF08-1128_v1.1.pdf .		Destruction	Denial of service
T-12.	Electromagnetic Interference	E, P	Disruption of electronic and wire transmissions could be caused by high frequency (HF), very high frequency (VHF), and ultra-high frequency (UHF) communications devices (jamming) or sun spots.			Denial of service
T-13.	Espionage	P	The illegal, covert act of copying, reproducing, recording, photographing or intercepting sensitive information.	Disclosure	Modification	
T-14.	Fire	E, P	Fire can be caused by arson, electrical problems, lightning, chemical agents, or other unrelated proximity fires.		Destruction	Denial of service
T-15.	Floods	E	Water damage caused by flood hazards can be caused by proximity to local flood plains. Flood maps and base flood elevation must be considered.		Destruction	Denial of service
T-16.	Fraud	P	Intentional deception regarding data or information about an information system could compromise the confidentiality, integrity, or availability of an information system.	Disclosure	Modification or destruction	Denial of service
T-17.	Hardware or Equipment Failure	E	Hardware or equipment may fail due to a variety of reasons.			Denial of service
T-18.	Hardware Tampering	P	An unauthorized modification to hardware that alters the proper functioning of equipment in a manner that		Modification	Denial of service

ID	Threat Name	Type Identifier	Description	Typical Impact to Data or System		
				Confidentiality	Integrity	Availability
			degrades the security functionality provided by the asset.			
T-19.	Hurricane	E	A category 1, 2, 3, 4, or 5 land falling hurricane could impact the facilities that house the information systems.		Destruction	Denial of service
T-20.	Malicious Software	P	Software that damages a system such a virus, Trojan, or worm.		Modification or destruction	Denial of service
T-21.	Phishing Attack	P	Adversary attempts to acquire sensitive information such as usernames, passwords, or SSNs, by pretending to be communications from a legitimate/trustworthy source. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to Web sites that appear to be legitimate sites, while actually stealing the entered information.	Disclosure	Modification or destruction	Denial of service
T-22.	Power Interruptions	E	Power interruptions may be due to any number of reasons such as electrical grid failures, generator failures, uninterruptable power supply (UPS) failures (e.g. spike, surge, brownout, or blackout).			Denial of service
T-23.	Procedural Error	U	An error in procedures could result in unintended consequences.	Disclosure	Modification or destruction	Denial of service
T-24.	Procedural Violations	P	Violations of standard procedures.	Disclosure	Modification or destruction	Denial of service
T-25.	Resource Exhaustion	U	An errant (buggy) process may create a situation that exhausts critical resources preventing access to services.			Denial of service

ID	Threat Name	Type Identifier	Description	Typical Impact to Data or System		
				Confidentiality	Integrity	Availability
T-26.	Sabotage	P	Underhanded interference with work.		Modification or destruction	Denial of service
T-27.	Scavenging	P	Searching through disposal containers (e.g., dumpsters) to acquire unauthorized data.	Disclosure		
T-28.	Severe Weather	E	Naturally occurring forces of nature could disrupt the operation of an information system by freezing, sleet, hail, heat, lightning, thunderstorms, tornados, or snowfall.		Destruction	Denial of service
T-29.	Social Engineering	P	An attacker manipulates people into performing actions, divulging confidential information, or providing access to computer systems or facilities.	Disclosure		
T-30.	Software Tampering	P	Unauthorized modification of software (e.g., files, programs, database records) that alters the proper operational functions.		Modification or destruction	
T-31.	Terrorist	P	An individual performing a deliberate violent act could use a variety of agents to damage the information system, its facility, and/or its operations.		Modification or destruction	Denial of service
T-32.	Theft	P	An adversary could steal elements of the hardware.			Denial of service
T-33.	Time and State	P	An attacker exploits weaknesses in timing or state of functions to perform actions that would otherwise be prevented (e.g., race conditions, manipulation of user state).	Disclosure	Modification	Denial of service
T-34.	Transportation Accidents	E	Transportation accidents include train derailments, river barge accidents, trucking accidents, and airline accidents. Local transportation accidents typically occur when airports, sea ports, railroad tracks, and major trucking routes occur in close proximity to systems facilities. Likelihood of HAZMAT cargo must		Destruction	Denial of service

ID	Threat Name	Type Identifier	Description	Typical Impact to Data or System		
				Confidentiality	Integrity	Availability
			be determined when considering the probability of local transportation accidents.			
T-35.	Unauthorized Facility Access	P	An unauthorized individual accesses a facility which may result in comprises of confidentiality, integrity, or availability.	Disclosure	Modification or destruction	Denial of service
T-36.	Unauthorized Systems Access	P	An unauthorized user accesses a system or data.	Disclosure	Modification or destruction	
T-37.	Volcanic Activity	E	A crack, perforation, or vent in the earth's crust followed by molten lava, steam, gases, and ash forcefully ejected into the atmosphere. For a list of volcanoes in the U.S. see: http://volcanoes.usgs.gov/about/volcanoes/volcanolist.php .		Destruction	Denial of service

4.4 Perform Risk Analysis

NIST identifies risk assessment as the first process in the risk management methodology. Organizations use the risk assessment to determine the extent of the potential threat and the risk associated with an information system. NIST defines **Risk** as "a function of the likelihood of a given threat-source's exercising a particular vulnerability and the resulting impact of the adverse event on the organization". The outcome of performing risk analysis yields risk exposure metrics that can be used to make risk-based decisions.

The FISMA risk analysis process is a qualitative risk analysis. In qualitative risk analysis, the risk level of exploiting a threat may be subjective and the justification for each risk is explained in terms of probability. The following tables have probabilities associated with the likelihood and the impact level of the risk. For example, when a system is easy to exploit, it has a "Very High" likelihood that a threat could exploit the vulnerability. Likelihood definitions and probabilities are in Table 10.

Note: The likelihood levels should not be confused or used interchangeably with the security categorization of the system even though they use the some of the same terminology. The security categorization is determined by the sensitivity of the data residing on the information system and is in the FIPS 199 publication.

Table 10: Likelihood Definitions from NIST 800-30 Rev. 1 Publication

Likelihood Probability Level	Description
Very Low	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
Low	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Moderate	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
High	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Very High	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.

Impact refers to the magnitude of potential harm to the information system (or its data) by successful vulnerability exploitation. Definitions for the impact are in Table 11. Since exploitation has not yet occurred, these values are perception values based on available information system information if the exploitation of a vulnerability can cause significant loss to a system (or its data) then the impact is "Very High".

Table 11: Impact Definitions from NIST 800-30 Rev. 1 Publication

Impact Probability	Description
Very Low	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.
Low	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals

Moderate	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
High	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Very High	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.

The combination of the Likelihood Probability and the Impact Probability creates the risk exposure. The risk exposure matrix shown in Table 12 presents the same likelihood and impact severity ratings as those found in *NIST SP 800-30 Rev. 1 Risk Management Guide for Information Technology Systems*.

Table 12: Risk Exposure Ratings from NIST 800-30 Rev. 1 Publication

Likelihood	Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Very Low	Very Low

Using Table 12 as a reference, Coalfire Federal Services reviewed all identified vulnerabilities and assigned a risk exposure located in the <System Acronym> SRTM in Appendix B.

Documenting the results of security control testing creates a record of the security posture for the system at a given moment in time. The record can be used by the AO to make risk-based decision and to create plans of action to mitigate unacceptable residual risks.

FISMA requires that a Plan of Action and Milestones (POA&M) be developed. The POA&M is a mitigation plan designed to address specific residual security risks and includes information on costing, resources, and target dates for remediation efforts resolving the identified security weaknesses. The plan is utilized as the primary mechanism for tracking all the residual risks and other issues. SSA will leverage the SAR to create a POA&M for <System Acronym>.

5 Security Assessment Results

This section describes all security risks found during assessment. The following elements for each security risk are reported.

- Identifier
- Name
- Source of Discovery
- Description
- Affected internet protocol (IP) Address/Hostname/Database
- Applicable Threats
- Likelihood (before mitigating controls/factors)
- Impact (before mitigating controls/factors)
- Risk Exposure (before mitigating controls/factors)
- Risk Statement
- Mitigating Controls/Factors
- Likelihood (after mitigating controls/factors)
- Impact (after mitigating controls/factors)
- Risk Exposure (after mitigating controls/factors)
- Recommendation

Below is a description of the SAR security risk elements.

- **Identifier:** All weaknesses are assigned a vulnerability identifier (ID) in the form of V#-Security Control ID. For example, the first vulnerability listed would be reported as V1-AC-2(2) if the vulnerability is for control ID AC-2(2). If there are multiple vulnerabilities for the same security control ID, the first part of the vulnerability ID must be incremented, for example V1-AC-2(2), V2-AC-2(2).
- **Name:** A short, unique name for each vulnerability.
- **Source of Discovery:** The source of discovery refers to the method that was used to discover the vulnerability (e.g., web application scanner, manual testing, security test procedure workbook, interview, document review). References must be made to scan reports, security test case procedure IDs, staff that were interviewed, manual test results, and document names. All scans reports are attached in Appendix C, Appendix D, Appendix E, and Appendix F. Results of manual tests can be found in Appendix G. If the source of discovery is from one of the security test procedure workbooks, a reference must point to the workbook name, the sheet number, and the cell number. Workbook tests results are found in Appendix B. If the source of discovery is from an interview, the date of the interview and the people who were present at the interview are named. If the source of discovery is from a document, the document must be named.

- **Description:** All security weaknesses must be described in enough detail to be reproduced by the stakeholder, the Information System Security Officer (ISSO), or the AO. If a test was performed manually, the exact manual procedure and any relevant screenshots must be included. If a test was performed using a tool or scanner, a description of the reported scan results for that vulnerability must be included along with the vulnerability identifier (e.g., Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), Nessus Plugin ID) and screenshots of the particular vulnerability being described. If the tool or scanner reports a severity level, that level must be reported in this section. Any relevant login information and role information must be included for vulnerabilities discovered with scanners or automated tools. If any security weaknesses affect a database transaction, a discussion of atomicity violations must be included.

- **Affected IP Address/Hostname(s)/Database:** For each reported vulnerability, all affected IP addresses/hostnames/databases must be included. If multiple hosts/databases have the same vulnerability, list all affected hosts/databases.

- **Applicable Threats:** The applicable threats describe the unique threats that have the ability to exploit the security vulnerability. (Use threat numbers from **Error! Reference source not found.**.)

- **Likelihood (before mitigating controls/factors):** Very High, High, Moderate, Low, or Very Low (see **Error! Reference source not found.**).

- **Impact (before mitigating controls/factors):** Very High, High, Moderate, Low, or Very Low (see **Error! Reference source not found.**).

- **Risk Exposure (before mitigating controls/factors):** Very High, High, Moderate, Low, or Very Low (see **Error! Reference source not found.**).

- **Risk Statement:** Provide a risk statement that describes the risk to the business. (See examples in **Error! Reference source not found.**). Also indicate whether the affected machine(s) is/are internally or externally facing.

- **Mitigating Controls/Factors:** Describe any applicable mitigating controls/factors that could downgrade the likelihood or risk exposure. Also indicate whether the affected machine(s) is/are internally or externally facing. Include a full description of any mitigating factors and/or compensating controls if the risk is an operational requirement.

- **Likelihood (after mitigating controls/factors):** Moderate or Low (see **Error! Reference source not found.**) after mitigating control/factors have been identified and considered.

- **Impact (after mitigating controls/factors):** Moderate or Low (see **Error! Reference source not found.**) after mitigating control/factors have been identified and considered.

- **Risk Exposure (after mitigating controls/factors):** Moderate or Low (see **Error! Reference source not found.**) after mitigating controls/factors have been identified and considered.

- **Recommendation:** The recommendation describes how the vulnerability should be resolved. Indicate if there are multiple ways that the vulnerability could be resolved or recommendation for acceptance of operational requirement.

5.1 Security Assessment Summary

<Two (2) vulnerabilities, (0 high, zero moderate, 2 low)> have been discovered as part of the manual security assessment testing. Vulnerability scans provided did not provide enough information to provide analysis of scan vulnerability to assessment result.

The vulnerabilities summary is contained in the following embedded file:

Table 13: Risk Exposure

T2 Risk Exposure Table.xlsx

<Embed applicable system's Risk Exposure table, EXAMPLE attached.>

6 Non-conforming Controls

In some cases, the initial risk exposure to the system has been adjusted due to either corrections that occurred during testing or to other mitigating factors. Additional detail is provided in the following sections.

6.1 Risks Corrected During Testing

Any risks that were discovered during the testing of the <System Acronym> subsystems and subsequently mitigated prior to authorization are listed in Table 14. Coalfire Federal Services verified risks corrected during testing. The verification method used to determine correction is noted in the right-hand column of Table 14.

Table 14: Summary of Risks Corrected During Testing

Identifier	Description	Source of Discovery	Initial Risk Exposure	Remediation Description	Date of Remediation	Verification Statement/Testing Procedures

6.2 Risks with Mitigating Factors

Risks that have had their severity levels changed due to mitigating factors are summarized in Table 15. The factors used to justify changing the initial risk exposure rating are noted in the right-hand column of the table. See Table 13 for more information on these risks.

Table 15: Summary of Risks with Mitigating Factors

Identifier	Description	Source of Discovery	Initial Risk Exposure	Current Risk Exposure	Description of Mitigating Factors

6.3 Risks Remaining Due to Operational Requirements

Risks that reside in the <system acronym> that cannot be corrected due to operational constraints are summarized in **Error! Reference source not found.**. An explanation of the operational constraints and risks are included in **Error! Reference source not found.** as well as in the appropriate security assessment test cases and SSP. Because these risks will not be corrected, they are not tracked in the POA&M. See **Error! Reference source not found.**for more information on these risks.

Table 16: Summary of Risks Remaining Due to Operational Factors

Identifier	Description	Source of Discovery	Current Risk Exposure	Operational Requirements Rationale

7 Risks Known for Interconnected Systems

Inherent relationships between the system and other interconnected systems may affect the overall system security posture. A summary of the risks known for systems that connect to <System Acronym> is provided in Table 17.

Table 17: Risks from Interconnected Systems

System	Authorization Date/Status	Date of POA&M	Control Family Identifier

8 Recommendations

<System Acronym> subsystem risks that were discovered during the assessment have an impact on the security posture of the SSA Federal Agency as a whole. These risks must be mitigated and Coalfire Federal Services has made recommendations in the Risk Exposure section, Table 14. These recommendations should be addressed by the SAM, system owners, OIS, and other stakeholders that have a responsibility for the controlling the overall risk of <System Acronym>.

Appendix A. Acronyms and Terms

Acronyms and terms used throughout this SAR are defined in Table 18.

Table 18: Acronyms and Terms

Acronym/Term	SAR Acronym Definitions
AC	Associate Commissioner
AC	Access Control
AO	Authorizing Official
ARB	Architecture Review Board
ART	Analysis and Reporting Tool
AU	Audit and Accountability
BRI	Benefit Rate Increase
BSM	Boundary Scope Memo
CA	Security Assessment and Authorization
CCB	Configuration Control Board
CIC	Customer Information Control System
CM	Configuration Management
CMP	Contingency Management Plan
COTR	Contract Officer's Technical Representative
CSAM	Cyber Security Assessment & Management
CSO	Component Security Officer
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DCS	Deputy Commissioner for Systems
DSPP	Division of Security Policy & PII
EPECS	Electronic Personal Enrollment Credential System
EPO	ePolicy Orchestrator
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
HRMIS	Human Resources Management Information System
HRODS	Human Resources Operational Data Store
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
ID	Identification

IP	Internet Protocol
ISCP	Information System Contingency Plan
ISO	Information Security Officers
ISP	Information Security Policy
ISSO	Information System Security Officer
LIS	Low Income Subsidy
NIST	National Institute of Standards and Technology
NSC	National Support Center
OIS	Office of Information Security
OMB	Office of Management and Budget
OSOHE	Office of Systems Operations and Hardware Engineering
OTSO	Office of Telecommunications and Systems Operations
PAM	Payment Application Modernization
PCCB	Project Configuration Control Board
PIN	Personal Identification Number
PIV	Personal Identification Verification
PL	Public Law
PL	(Control) Planning
PM	Program Manager
POA&M	Plan of Action and Milestones
PRIDE	Project Resource Guide
PS	(Control) Personnel Security
P, U, E	Purposeful, Unintentional, Environmental
SA	System and Services Acquisition
SAM	Security Authorization Manager
SAP	Security Assessment Plan
SARA	Security Administration Report Application (User Guide)
SAR	Security Assessment Report
SC	Systems and Communications Protection
SDLC	System Development Life Cycle
SI	System and Information Integrity
SMACS	Security Management Access Control Systems
SO	System Owner
SOC	Security Operation Division

SP	Special Publication
SRC	System Release Certificate
SRTM	Security Requirements Traceability Matrix
SSA	Social Security Administration
SSC	Secondary Support Center
SSP	System Security Plan
SVR	Security Violations Report
Threat	An adversarial force or phenomenon that could affect the availability, integrity, or confidentiality of an information system, its networks, and the facility that houses the hardware and software.
Threat Actor	An entity that initiates the launch of a threat agent is referred to as a threat actor.
Threat Agent	An element that provides the delivery mechanism for a threat.
UPS	uninterruptable power supply
USC	United States Code
Vulnerability	An inherent weakness in an information system that can be exploited by a threat or threat agent, resulting in an undesirable impact in the protection of the confidentiality, integrity, or availability of the system (application and associated data).

Appendix B. Security Risk Traceability Matrix (SRTM)

The Security Risk Traceability Matrix (SRTM) with test results and test procedures are within the following embedded document in Table 19.

Table 19: Security Test Procedure Workbook

T2 SRTM Worksheet.xlsx

<Embed the applicable system's Security Risk Traceability Matrix (SRTM), EXAMPLE attached.>

Appendix C. Infrastructure Scan Results

The Nessus scanner along with the McAfee ePolicy Orchestrator (EPO) deployed by the SOC was used to scan SSA servers. Associated Windows Database servers that have the EPO agent deployed within the <System Acronym> boundary were scanned. The other <System Acronym> servers did not have any vulnerability scanning tools available, which allowed for scanning of mainframe or storage hardware, and therefore were not scanned.

Infrastructure Scans: Inventory of Items Scanned

Table 20 provides an inventory of infrastructure items scanned during this assessment.

Table 20: Inventory of Items Scanned

T2 Scanned Inventory Items.xlsx

<Embed the applicable system's Inventory of Items Scanned, EXAMPLE attached.>

Infrastructure Scans: Raw Scan Results

Table 21 has the <System Acronym> raw scan results:

Table 21: Raw Scan Results

T2 Raw Scan Results.xlsx

<Embed the applicable system's Raw Scan Results, EXAMPLE attached.>

Infrastructure Scans: False Positive Reports

Table 22 provides a list of false positive reports collected during infrastructure scans if applicable.

Table 22: Infrastructure Scans: False Positive Reports

ID#	IP Address	Scanner Severity Level	Finding	False Positive Explanation

Appendix D. Database Scan Results

Database scan results are included in this appendix.

Database Scans: Inventory of Databases Scanned

Table 23 provides an inventory of any databases scanned during this assessment if applicable.

Table 23: Inventory of Databases Scanned

IP Address	Hostname	Software and Version	Function	Comment

Database Scans: False Positive Reports

Table 24 provides a list of false positive reports collected during database scans if applicable.

Table 24: Database Scans: False Positive Reports

ID#	IP Address	Scanner Severity Level	Finding	False Positive Explanation

Appendix E. Web Application Scan Results

Web application scan results are included in this appendix.

Web Application Scans: Inventory of Web Applications Scanned

Table 25 provides an inventory of all web applications scanned during this assessment if applicable.

Table 25: Inventory of Web Applications Scanned

Login URL	IP Address of Login Host	Function	Comments

Web Application Scans: False Positive Reports

Table 26 provides a list of false positive reports collected during web application scans if applicable.

Table 26: Web Application Scans: False Positive Reports

ID#	IP Address	Scanner Severity Level	Finding	False Positive Explanation

Appendix F. Assessment Results

Assessment results are summarized in Table 27.

Table 27: Summary of System Security Risks from FISMA Testing

Risk Level	Assessment Test Cases	Total
High	<# high risks>	<% of total risks>
Moderate	<# moderate risks>	<% of total risks>
Low	<# low risks>	<% of total risks>
Operationally Required	<# operationally required high risks>	<% of total risks>
Total	<Sum of all H, M, L risks>	100%

✍ **NOTE:** Total is the sum of high, moderate, and low risks with operationally required risks being represented as a subset of this total.

Appendix G. Penetration Test Report

<Update the text below to reflect actual penetration test results for this assessment. Embed the penetration test report as appropriate.>

Coalfire Federal Services is not authorized as per the Statement of Work (SOW) to perform a formal Penetration Test for the <System Acronym> Batch and Internet Services subsystems. Therefore, no data from a penetration test is available for this assessment.

Appendix H. Security Assessment Report Signature

Table 28: SAR Signatures

Acceptance and Signature	
I have read the above Security Assessment Report prepared by the third party assessment organization, Coalfire Federal Services. I acknowledge the assessment was completed as per the <System Acronym> SAP and understand the findings detailed herein.	
Security Authorization Manager/ <SAM>:	
OIS Division of Compliance and Assessments Director: <DD>	

EXHIBIT D

Social Security Administration (SSA)

Security Categorization: <Enter Categorization>

Risk Assessment Report (RAR)

FOR

<System Name> (<Acronym>)

<DRAFT/FINAL> Version <x.x>

<Month DD, YYYY>

Prepared by

Office of Information Security

<INSTRUCTIONS: Orange, bracketed text indicates instructions on how a section should be completed or sample text, which should be replaced with project specific information or removed. Ensure sample text is turned from orange to black where necessary (e.g., headings shall be changed to the standard heading color), and all instructions are removed (including this paragraph). All black text shall remain unchanged.>

Document Revision History

Revision History	Date	Summary of Changes	Author
1.0	<Month DD, YYYY>	Initial release	<name>
<x.x>	<Month DD, YYYY>	<description>	<name>
<x.x>	<Month DD, YYYY>	<description>	<name>

Table of Contents

List of Tables

1 Risk Assessment Report (RAR) Background

The Office of Management and Budget (OMB) directive requires the Social Security Administration (SSA) to assess and re-authorize its major information technology (IT) systems at least once every three years and in the event of a major change, when that change occurs. This information must be reported in the annual Federal Information Security Modernization Act (FISMA) report to OMB and Congress during the fourth quarter (Q4) of each year. OMB has directed Chief Information Officers (CIO) of Federal agencies to follow the guidance found in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, to assess and re-authorize their information systems. This security authorization process contains subordinate efforts including performing risk-based reviews of the systems, developing/updating system security plans (SSP), and assessing and testing the security controls implemented for SSA's information systems.

2 RAR Executive Summary for <System Name>

The Office of Information Security (OIS) contracted with Coalfire Federal Services, a third party assessment organization (3PAO), to conduct a system specific risk assessment on <system name> (<ACRONYM>). The acting Director of the Division of Compliance and Assessments, and the Security Authorization Manager (SAM) of <SYSTEM ACRONYM> approved the controls selected for this risk assessment. Thirty-two (32) controls were tested over eleven (11) different NIST 800-53 Rev 4 control families. These controls were selected out of the <system categorization> baseline due to <SYSTEM ACRONYM> being categorized as a <system categorization> system as per the FIPS 199. During the assessment, there were <55 manual tests conducted, 62 interviews, and 84 document examinations>. Each of these is a requirement of a specific control. At the conclusion of the assessment, two controls were identified as "not implemented". It should be noted that these controls have since been identified as common and should be added to the common control list. The controls that were not implemented, identified as PS4 (personnel termination), and PS 5 (personnel transfer), requires the SSA Information Security Policy (ISP) to document specific exit interview security debrief policies and procedures and the defined time period in which these must be carried out. Please refer to Table 5 for specific details. The likelihood of these vulnerabilities being exploited combined with the potential system impact is considered an overall **LOW** risk to the system. It is recommended that the <system name> assigned representative from the Security Assessment and Authorization Branch (SAAB) work with the System Authorization Manager (SAM) to mitigate these risks. Due to the overall identified risk being LOW, it is recommended that this be considered an acceptable risk and the system be given an authority to operate (ATO) for the next three years.

3 <system name> System Purpose

The <system name> (<ACRONYM>) system, has a <system categorization> Security Categorization. The boundaries are designed to aid SSA in the accomplishment of its mission to provide cost-effective and reliable services to other Federal agencies, and the public at large.

<Insert detailed information>

Coalfire Federal Services' objective is to provide IT Independent Verification and Validation (IV&V) Support Services for <SYSTEM ACRONYM>.

3.1 System Name/Title/Unique Identifier

System/Application Name: <system name> (<SYSTEM ACRONYM>)

Unique Identifier : <016-00-SSA/DCS-M-001>

3.2 Responsible Organization

Table 1: <SYSTEM ACRONYM> Points of Contact


Title II Batch POCs.xlsx


Title II Internet Applications POCs.xlsx

<Embed the applicable system's POCs, EXAMPLE attached.>

3.3 Security Categorization

This authorization boundary has been categorized as **<system categorization>** risk according to FIPS 199. Refer to Table 5 below for supporting documentation regarding the determination of the application's security categorization.

Table 2: <System Name> Security Categorization

Information Type	Confidentiality	Integrity	Availability
Accounting *Mission Area:* Financial Management Explanation: Selected risk values derived from NIST SP-800-60, and FIPS 199, considering SSA business case.	L	M	L
Payments Mission Area: Financial Management Explanation: Selected risk values derived from NIST SP-800-60, and FIPS 199, considering SSA business case.	L	M	L
Reporting & Information *Mission Area:* Financial Management Explanation: Based on the protection requirements for confidentiality, integrity and availability, the overall system sensitivity is <SYSTEM CATEGORIZATION>. The loss, misuse or unauthorized access to Agency data can be expected to have a serious adverse effect on SSA operations and assets.	L	M	L
Entitlement Event Information *Mission Area:* General Government Explanation: Selected risk values derived from NIST SP-800-60, and FIPS 199, considering SSA business case.	M	M	M
Personal Identity and Authentication *Mission Area:* General Government	M	M	M
Information Sharing *Mission Area:* Information and Technology Management Explanation: Selected risk values derived from NIST SP-800-60, and FIPS 199, considering SSA business case.	N/A	N/A	N/A
Overall	**M**	**M**	**M**

4 Risk Assessment Approach

4.1 Risk Assessment Purpose

The purpose of this Risk Assessment Report (RAR) is to summarize the residual risk identified during the security assessment of <SYSTEM ACRONYM>. Risk is a factor derived from a vulnerability that can be exploited and the likelihood that it will be exploited. Please see Appendix A for the NIST 800-60 Volume II publication for the definition of risk.

4.2 Risk Assessment Objective

The objective of the risk assessment is to identify any controls that are not fully implemented as required by FISMA. Controls that are not implemented pose a measureable risk to SSA and that risk must be mitigated in a timely manner based on the level or risk the non-implemented control creates. For example, a low risk may only require an update to a policy or a POA&M that the system's SAM must execute. Another example is a High risk that must have immediate action taken by the SAM and other stakeholders in order to prevent a threat actor(s) from exploiting the discovered risk.

4.3 Risk Assessment Scope

The previous system specific risk assessment was conducted on <SYSTEM ACRONYM> in <date>. The residual risk was identified and submitted to the SSA's CIO. This submission was in accordance with OMB and FISMA guidelines to present the risk level of <SYSTEM ACRONYM> and ask for the ATO <SYSTEM ACRONYM> for the next three years. The CIO granted the ATO on <Month DD, YYYY> and allowed <SYSTEM ACRONYM> to operate from <Month DD, YYYY> to <Month DD, YYYY>.

A new risk assessment is required by OMB and FISMA in order to identify the current residual risk and any risks associated with controls that are not fully implemented. The assessed controls were selected based on the <SYSTEM ACRONYM> Security Assessment Plan (SAP) approved by the OIS Director and the <SYSTEM ACRONYM> SAM.

In addition to the controls selected, SSA uses the Nessus scanner along with the McAfee ePolicy Orchestrator (EPO) deployed by the SOC to look for signature based vulnerabilities in accordance with the SSA ISP. Associated Windows Database servers that have the EPO agent deployed within the <SYSTEM ACRONYM> boundary were scanned. The other <SYSTEM ACRONYM> servers did not have any vulnerability scanning tools available that could scan mainframe or storage hardware, and therefore were not scanned.

The risk assessment was performed in accordance with all applicable laws, regulations, rules and orders of all governmental agencies and authorities. A complete list of referenced publications and regulations can be found in Appendix A. All risks associated with <SYSTEM ACRONYM> that were identified during the assessment and the potential impact of those risks are documented in this RAR.

The RAR complies with the following SSA guidance:

- SSA ISP

4.4 Limitations

The <SYSTEM ACRONYM> subsystems, which reside within the National Support Center (NSC), rely on the Office of Systems Operations and Hardware Engineering (OSOHE) for hardware, software, and maintenance support. Additionally, user access and user profile provisioning for <SYSTEM ACRONYM> subsystems residing on the mainframe, are provided by CA Top Secret, and managed by the Office of Systems Operations and Hardware Engineering (OSOHE), not by <SYSTEM ACRONYM>. Therefore, some access controls specific to <SYSTEM ACRONYM> are tested during an enterprise level common control assessment, and not during the <SYSTEM ACRONYM> system specific assessment reported within this RAR.

This assessment was limited to the 32 system specific controls as listed in the approved SAP.

4.5 Risk Assessors

The participants in this risk assessment included the following Coalfire Federal Services personnel:

Table 3: Assessment Team Points of Contact

Name	Role	Contact Information
<TJ Crews>	Program Manager	<Tj.crews@ssa.gov>
<Kenneth Free>	Lead Assessor (Senior Analyst)	<kenneth.free@ssa.gov>
<Gregory Bonham>	Junior Assessor	<gregory.bonham@ssa.gov>
<Thomas G. Volpe, Sr.>	Lead Assessor (Surge Support)	<Thomas.G.Volpe@ssa.gov>

The following techniques and NIST/FIPS publications were used to gather information relevant to the <SYSTEM ACRONYM>:

- **NIST SP 800-60 Volume II Revision 1/ and FIPS 199.** The Risk Assessment (RA) Team utilized the <SYSTEM ACRONYM> Security Categorization, dated February 16, 2017 to determine associated system security categorization for the <SYSTEM ACRONYM>. System security categorization determines which recommended set of minimum (baseline) security controls from NIST SP 800-53 Revision 4 must be implemented.
- **NIST SP 800-53 Revision 4.** The RA Team utilized NIST SP 800-53 Revision 4 to determine the recommended set of minimum-security controls. The security controls (management, operational, and technical safeguards or countermeasures) were reviewed to ensure they adequately protect the confidentiality, integrity, and availability of the <SYSTEM ACRONYM>, and that the selected security controls have been implemented, or there is a plan for future implementation.
- **Interviews.** Interviews were conducted on-site with the SAM, System Administrator, and Database Administrator by the RA Team to collect useful information about the <SYSTEM ACRONYM>. Follow-up communications were conducted via email and by telephone to collect additional information about the <SYSTEM ACRONYM>.
- **Examination/Document Reviews.** The RA Team reviewed documentation from the SSA for <SYSTEM ACRONYM>, such as policy and implementation guidance. POA&M, and the prior Security Assessment and Authorization (SA&A) Package, including the previous SSP, Risk Assessment, and the Security Control Assessment (SCA) Plan were reviewed.
- **Testing of Systems.** Testing and Evaluation of security controls for <SYSTEM ACRONYM> was based on System Specific and Hybrid security controls defined by the OIS Rev4 SSA Control Inheritance Structure Worksheet with a <SYSTEM CATEGORIZATION> Baseline. Using the NIST Guidance from NIST SP 800-53A Revision 4, the RA Team tested and evaluated these controls for specified conditions that compare actual with expected behavior, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.

4.6 Results

The overall risk level of the <SYSTEM ACRONYM> was determined to be ***Low,*** which is the combination of the likelihood of identified threats being able to exploit known system vulnerabilities and the potential the impact to <SYSTEM ACRONYM>.

Low risk indicates that corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time. The preliminary review of security measures for the protection of the <SYSTEM ACRONYM> identified two low threat-vulnerability pairs (risks) in the overall risk assessment as summarized below in Table 2.

Table 4: Overall Risk Level

Risk Rating	Control Category			
	Management	Operational	Technical	Total
Very High	0	0	0	0
High	0	0	0	0
Moderate	0	0	0	0
Low	2	0	0	2
Very Low	0	0	0	0
Total	**2**	**0**	**0**	**2**

4.7 Recommendation

It is the recommendation from the Office of Information Security that an issuance of an Authority to Operate (ATO) for <system name> (<ACRONYM>) be given. This recommendation comes from the assessment findings from the 3PAO that conducted a system specific security assessment. The overall security categorization of <SYSTEM ACRONYM> is <system categorization> and the findings have an overall risk of **LOW.**

5 Summary of Findings

Table 5: <SYSTEM ACRONYM> Results Summary

Item No.	Finding (In Order by Control Family)	Threat Source	Likelihood Level	Impact Level	Risk Level	Recommended Corrective Action(s)
V-1	**PS-4.c.1** **PS-4.c.2** **Personnel Termination** SSA ISP does not define the security debrief topics or policy to discuss with separating employees. In addition, the SSA ISP has no policy, guidelines for including the security debrief actions, or SSA specific information security topics during the exit interview as defined in PS-4.c.1 and PS-4.c.2.	Insider Threat with Intent (e.g., Poorly Trained, Disgruntled, Malicious, Negligent, Dishonest, or Terminated Employees) Insider Threat without Intent or Knowledge Computer Crime/Hackers Espionage (e.g., Companies, Foreign Governments, or Other Government Interests)	Low	Low	Low	This is an agency requirement that must be reflected in the SSA ISP and is the responsibility of Division of Security Customer Service (DSCS). The Security Authorization Manager (SAM) is not responsible for updating policy. The SSA ISP should be updated to include a requirement that employees sign a Non-Disclosure Agreement (NDA), and have a security debrief to discuss the importance of not disclosing knowledge of specifics pertaining to the SSA information system environment. The ISP section 2.1.1.3 should be updated to reflect this. In addition, section 2.1.1.3 should be updated to reflect that a security debrief must be included as part of the exit interview. Exit interview guidance is currently located here: http://personnel.ba.ssa.gov/OPE/cpps/exitprocedures.html

Item No.	Finding (In Order by Control Family)	Threat Source	Likelihood Level	Impact Level	Risk Level	Recommended Corrective Action(s)
V-2	**PS-5.b.1** **PS-5.b.2** **Personnel Transfer** SSA ISP does not define what security actions are to be taken when an employee is transferred or reassigned. The SSA ISP also does not specify the time period in which security actions that are defined in must occur.	Insider Threat with Intent (e.g., Poorly Trained, Disgruntled, Malicious, Negligent, Dishonest, or Terminated Employees) Insider Threat without Intent or Knowledge	Low	Low	Low	This is an agency requirement that must be reflected in the SSA ISP and is the responsibility of DSCS. The ISP section 2.4 should be updated to define what security actions need to occur, in what period of time and what personnel or role is to be identified to be notified when an employee is transferred or reassigned.

Authority To Operate (ATO) Recommendation

Acceptance and Signature	
As the Security Authorization Manager (SAM) for <system name>, I hereby certify that this Risk Assessment Report provides an accurate representation of the system and its subsystems that were assessed. I also certify that it is my recommendation based on the findings that the SSA Chief Information Officer (CIO) grant an Authority to Operate (ATO) for <system name> for the next three (3) years.	
Security Authorization Manager: <name>	
As the Acting Director of the Division of Compliance and Authorization (DCA) in the Office of Information Security (OIS), I hereby certify that this Risk Assessment Report provides an accurate representation of the system and its subsystems that were assessed. I also certify that it is my recommendation based on the findings that the SSA Chief Information Officer (CIO) grant an Authority to Operate (ATO) for <system name> for the next three (3) years.	
Division of Compliance and Assessments Director Steven Harkness (Acting)	

Table 6: Acronym List

Acronym	Definition
AO	Authorizing Official
BSM	Boundary Scope Memorandum
CET	Customer Engagement Tool
CICS	Customer Information Control System
CIO	Chief Information Officer
CSO	Component Security Officer
DCA	Division of Compliance and Authorization
DCS	Deputy Commissioner for Systems
EPO	McAfee ePolicy Orchestrator
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FOUO	For Official Use Only
ISA	Interconnection Security Agreement
ISP	Information Security Policy
IT	Information Technology
IV&V	Independent Verification and Validation
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LIS	Low Income Subsidy
MKS	Mortise Kern Systems
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NDA	Non-disclosure Agreement
NSC	National Support Center
NIST	National Institute of Standards and Technology
OIS	Office of Information Security
OMB	Office of Management and Budget
OSOHE	Office of Systems Operations and Hardware Engineering
OTSO	Office of Telecommunications and System Operations
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
PSC	Program Service Centers
RA	Risk Assessment or Risk Assessor

Acronym	Definition
RAR	Risk Assessment Report
RSDI	Retirement, Survivor, or Disability Insurance
SA&A	Security Assessment and Authorization
SAM	Security Authorization Manager
SAP	System Assessment Plan
SBU	Sensitive But Unclassified
SCA	Security Control Assessment
SO	System Owner
SP	Special Publication
SSA	Social Security Administration
SSP	System Security Plan
VPN	Virtual Private Network
3PAO	Third Party assessment Organization

APPENDIX A. REFERENCE DOCUMENTS

The following documents were reviewed during the risk assessment process of the SSA's security controls:

- Federal Information Processing Standard (FIPS) 199
- NIST Special Publication 800-30 Rev. 1, "Guide for Conducting Risk Assessments"
- Office of Management and Budget (OMB) Circular A-130.
- NIST Special Publication 800-39
- NIST Special Publication 800-60 Revision 1, Volumes 1&2
- NIST Special Publication 800-53 Revision 4
- SSA Information Security Policy (ISP)

EXHIBIT E

Social Security Administration (SSA)

Security Categorization: <Enter Categorization>

NOTE: The Security Categorization for the system may not be available at the time of the development of this document if the system is a newly developed system or has undergone a major change which has augmented the data types processed by the system. Additional information on completing the security categorization of the information system can be found on the DSPP website at: http://sharepoint.ba.ssa.gov/DCS/OIS/DSPP/Veris%20TO14%20IVV%20and%20OA/Forms/AllItems.aspx?RootFolder=%2fDCS%2fOIS%2fDSPP%2fVeris%20TO14%20IVV%20and%20OA%2fIVV%2fTEMPLATES%2fOIS%20TEMPLATES%20FY16&FolderCTID=0x0120003BC3DC1169B0CE47BB662BC248F5B5EE.

<Document Name>

FOR

<Externally Hosted Information System Name>

<(Acronym)>

<DRAFT/FINAL> Version <X.X>

<Month DD, YYYY>

Prepared by

[COMPANY LOGO]

[COMPANY STREET ADDRESS]

[COMPANY CITY, STATE ZIP]

Document Revision History

Revision Number	Revision Date	Page Number	Revision Summary	Name of Reviewer
V[X.X]	MM/DD/YYYY	All/Page No.	[E.g. Initial Draft, Annual Review, etc.]	[Company/Agency Name: Contact Name]

PREFACE

To carry out its wide-ranging responsibilities, the Social Security Administration (SSA), and its employees and managers have access to diverse and complex automated information systems, which includes, file servers, local and wide area networks (LANs/WANs) running on various platforms, and telecommunications systems. The components and offices within the SSA depend on the confidentiality, integrity, and availability (as defined by the Federal Information Processing Standard (FIPS) 199) of these systems and their data in order to accomplish day-to-day operations.

In accordance with Office of Management and Budget (OMB) Circular A-130, Appendix III, all federal systems have value and require some level of protection. The generic term "system" is used to mean either a general support system or a major application. (See NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems* for additional information).

EXECUTIVE SUMMARY

The SSA relies on its information technology (IT) systems, including the [Enter SYSTEM NAME (Acronym)], to accomplish its undertaking of providing cost-effective and reliable services to the SSA, other Federal agencies, and the public at large. Since this externally hosted information system is part of an SSA security authorization boundary, it is subject to meet some or all of the SSA specific security requirements depending upon the information it processes and the services it provides for the SSA.

[Provide an EXECUTIVE SUMMARY and overview of the information system. This summary should describe what the information system is, what its importance is to SSA, who is in the user audience, and any additional subsystems that is encompassed in the system.]

The purpose of this system security plan is to provide an overview of the security requirements of the [ENTER SYSTEM NAME HERE] system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system.

The SSP documents the structured process of planning adequate, cost-effective security protection for a system. It shall reflect input from various managers/stakeholders with responsibilities concerning the system from the hosting company and from the SSA component for which the system provides services.

> [Note: This SSP template shall be used to document an external hosted Information Systems that "IS" associated with one of the existing SSA Security Authorization Boundaries.

As part of the development of this SSP document, the external system ISO or designee along with the SSA SAM and the Office of Information Security (OIS) will need to follow the instructions to determine which new application/system/sub-system should be included or associated with SSA. See section 1.1 below for more details related to this process.] ← DELETE THESE INSTRUCTIONS UPON COMPLETION

SYSTEM SECURITY PLAN AGREEMENT SUMMARY

This SSP documents a formal agreement among the organizational officials approving the security controls designed to meet the security requirements for the [SYSTEM NAME]. These officials are the SSA System Owner (SO), (External Contractor) Information System Security Officer (ISSO), SSA Security Authorization Manager (SAM) and the SSA Authorizing Official (AO).

Each organizational official has signed this agreement summary for the reasons identified below and has concurred with the security category of this Controlled Unclassified Information (CUI) system to be [LOW/MODERATE]. *See Executive Order 13556 for more information on CUI*.

[Check the box below that is applicable ← DELETE]

☐ **Initiation of the System Security Plan (including FIPS 199 security categorization)**[1]

☐ **Annual Update of the System Security Plan (no significant changes)**

Acceptance and Signature	
As the Designated Representative(s) for <System Name>, I hereby certify that the <System Acronym> System Security Plan described in this document provides an accurate representation of the <System Acronym> and its subsystems.	
SSA Security Authorization Manager [ENTER NAME OF SAM ← DELETE	<Insert digital signature>
SSA DSP Director [ENTER NAME OF DSP DIRECTOR] ← DELETE	<Insert digital signature>

[1] When there are no significant changes, the System Owner, Information System Security Officer and SSA Security Authorization Manager must sign the agreement summary for an annual update. The Authorizing Official is not required to sign if there are no significant changes affecting the security posture of the system requiring reauthorization. Reauthorization is addressed via a formal memorandum approving the security plan and authorizing the system to operate for a specified period of time.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1 Information System Identification

1.1 Determination of System

Table 1: System Name/Identifier

System Name/Title:	System ID No:
<System name: external information system name> (short name-subsystem short name)	

1.2 Responsible Organization

Table 2: Responsible Organization

Organization	Address

1.3 Information System Categorization

Security categorizations are to be performed as the first step in the security authorization process as required by Federal Information Processing Standard (FIPS) 199 in order to select appropriate system security controls to be addressed throughout the rest of the security authorization. FIPS 199 categories are derived according to the potential impact on the agency that would occur if its Confidentiality, Integrity, or Availability were compromised. FIPS 199 category definitions are as follows:

- **High Impact:** The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
- **Moderate Impact:** The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. (*At SSA, the highest security categorization is currently Moderate*)
- **Low Impact:** The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Based on the system categorization of this externally hosted system the [SYSTEM ACRONYM] system has been categorized as a **[LOW/MODERATE]** system according to FIPS 199.

[Enter an "X" in the applicable section] ← DELETE

Table 3: Security Categorization

Low	☐
Moderate	☐

1.4 General Description of Information Sensitivity

Sensitive information is defined by the Computer Security Act (section 552a of Title 5, United States Code) as any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled. The National Institute of Standards and Technology (NIST) Special Publication 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* further defines the requirements for Personal Identity Information (PII) which SSA follows with regard to protecting its sensitive PII.

FIPS 199 defines security categories for information systems based on potential impact on organizations, assets, or individuals should there be a breach of security—that is, a loss of confidentiality, integrity, or availability. FIPS 199 security categories play an important part in defining information system security boundaries by partitioning the agency's information systems according to the criticality or sensitivity of the information and information systems and the importance of those systems in accomplishing the agency's mission. This is particularly important when there are various FIPS 199 impact levels contained in one information system. The FIPS 199 requirement to secure an information system to the high watermark or highest impact level must be applied when grouping minor applications/subsystems with varying FIPS 199 impact levels into a single general support system or major application unless there is adequate boundary protection, e.g., firewalls and encryption, around those subsystems or applications with the highest impact level. Additionally, there must be assurance that the shared resources, i.e., networks, communications, and physical access within the whole general support system or major application, are protected adequately for the highest impact level. Having the ability to isolate the high impact systems will not only result in more secure systems, but will also reduce the amount of resources required to secure many applications/systems that do not require that level of security. NIST SP 800-53 provides three security control baselines, i.e., low, moderate, and high (high is not addressed by this SSP), that are associated with the three FIPS 199 impact levels; as the impact level increases, so do the minimum assurance requirements. For reporting purposes, i.e., FISMA annual report, when an information system has varying FIPS 199 impact levels, that system is categorized at the highest impact level on that information system.

1.5 Impact Level for Information Types

The following tables identify the information types that are input, stored, processed, and/or output from **[System Acronym]**. The selection of the information types is based on guidance provided by OMB Federal Enterprise Architecture Program Management Office Business Reference Model 2.0 (http://www.whitehouse.gov/omb/e-gov/fea), and the FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems,* and NIST Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories.* SP 800-60 includes two volumes: Volume I is a basic guideline and Volume II contains appendices. Users should review the guidelines provided in Volume I, then refer to only the material from the appendices that is applicable. NIST SP 800-60 is available for download at http://csrc.nist.gov/publications/.

The potential impact is ***LOW*** if—

> The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
>
> A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is ***MODERATE*** if—

The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is ***HIGH*** if—

The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

[List the different information types per NIST SP 800-60 and indicate provisional impact level. Add or modify information types if necessary]. This information can be copy/pasted from the SSA Parent System FIPS199 Security Categorization Review documentation, Section 4. ← DELETE THESE INSTRUCTIONS UPON COMPLETION

Table 4: Impact Level for Information Types

NIST Information Type	NIST SP 800-60, Volume II Reference	NIST Recommended Provisional Impact Levels			System Owner Selected Impact Levels			Comments
		Confidentiality	Integrity	Availability	Confidentiality	Integrity	Availability	
EXAMPLE: Personal Identity and Authentication Information Type	C.2.8.9	M	M	M	M	M	M	None

1.6 System Points of Contact

<Complete the attached spreadsheet with system specific information.>

Table 5: <System Name> Points of Contact

SSP-Point of Contacts.xlsx

1.7 Assignment of Security Responsibility

Table 6: [System Acronym] (Contractor) Information System Security Officer (ISSO)

Name:	
Title:	
Agency:	
Address:	
Telephone:	
Email:	
Responsibility:	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program. Information System Security Officer (ISSO).

Table 7: SSA Security Authorization Manager (SAM)

Name:	
Title:	
Agency:	
Address:	
Telephone:	
Email:	
Responsibility:	SSA Security Authorization Manager

1.8 System Operational Status

The [SYSTEM ACRONYM] and its component systems are in the [INITIATION, ACQUISITION/DEVELOPMENT, IMPLEMENATION, OPERATIONAL/MAINTENANCE] phase of their System Development Life Cycles (SDLC).

[Enter an "X" in the applicable section] ← DELETE

Table 8: Information System Operational Status

Initiation	Development	Implementation	Operational

1.9 Information system Type

[Enter an "X" in the applicable section below] ← DELETE

Table 9: Information System Type

Subsystem/Application	Major Application	General Support System

1.10 Security Status

[SECURTIY AUTHORIZATION ACRONYM/ EXTERNAL INFORMATION SYSTEM ACRONYM] received a full Authority to Operate (ATO) on [Enter DATE of ATO].

1.11 General Description and Purpose

[This section should contain a detailed general description and overall purpose for the information system. It should identify the system's purpose, capabilities, users, arrangements for hosting, connection and/or interface to SSA, and information data flow; discuss the hardware, software and firmware implemented in support of the information system] ← DELETE

1.12 Data Types

Table 10: NIST SP 800-60 Vol 2. Information Data Types

NIST Information Type	NIST SP 800-60, Volume II Reference	Data Type Description
EXAMPLE: Personal Identity Information Type	C.2.8.9	Personal identity and authentication information includes that information necessary to ensure that all persons who are potentially entitled to receive any federal benefit are enumerated and identified so that Federal agencies can have reasonable assurance that they are paying or communicating with the right individuals. This information include individual citizen's Social Security Numbers, names, dates of birth, places of birth, parents' names, etc.

1.13 Information System Boundary

The [SYSTEM ACRONYM] system architecture, environment and agreement boundary is described below.

1.14 System Architecture/Environment

[Provide a description of the information system architecture/environment, explaining where and by whom it is hosted, whether it is a web-based (or cloud, etc.) application, what Software (SW) it is utilizing, what SW sits on the front end, back end, OS, how many users access the system, describe user interfaces, and designate whether connectivity to SSA and/or the outside is through VPN or WAN, etc.] ← DELETE

[INSERT a diagram of the information system architecture, including its connections/interfaces/other relationships to SSA]. ← DELETE

Figure 1: [System Acronym] Architecture Diagram

1.15 Security Authorization Boundary

[Provide information of where the information system is located; where backups and restores are conducted, and specifically where databases are housed. Provide an explanation of where the servers are located (company facility, datacenter, etc.), personnel, public access or not, how the systems are connected, how remote users can connect and how in and outbound internet connections are secured and maintained]. ← DELETE

[INSERT a diagram of the information security authorization boundary showing its connections/interfaces/other relationships to SSA.]← DELETE

Figure 2: [System Acronym] Accreditation Boundary

1.16 System Inventory

The hardware (HW) and software (SW) components included in the externally hosted, non-SSA [System Acronym] boundary are listed in the tables below. <System acronym> consists of multiple technologies. Table 11 contains a listing of technologies (hardware, software, technologies and platforms) that reside within the <system acronym> authorization boundary. Technology is listed per system and subsystem:

<Complete the embedded spreadsheet with system specific information.>

Table 11: Inventory: List of Technologies

Table 6_Inventory -
List of Technologies -

NOTE: Any changes to the scope of the Authorization Boundary after the Boundary Scope Meeting and finalization of the BSM may impact the overall IV&V schedule.

1.17 System Interconnections

The externally hosted [SYSTEM ACRONYM] requires that written agreements (e.g., Memorandums of Understanding (MOUs), Memorandums of Agreement (MOAs), Interconnection Security Agreements (ISAs), etc., on the security controls to be enforced on interconnecting systems and must be obtained prior to connecting and/or sharing sensitive data/information. Table 18 shows the status of these agreements between [SYSTEM ACRONYM] and the external systems that share its information. [SYSTEM ACRONYM] [Has /does not have] external communications requiring MOUs or ISAs.

Table 12: [System Acronym] System Interconnections

Information System	Organization	Type (GSS/MA)	Agreement (ISA/MOU/MOA)	Date	FIPS 199 Category	C&A Status	DAA
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

2 [System Acronym] NIST SP 800-53 - Rev 4 MINIMUM SECURITY CONTROLS

The minimum security control baseline for [LOW/MODERATE]-impact systems from NIST SP 800-53 Revision 4 is documented below. Specifically, this section provides a description of how all the minimum-security controls in the baseline are being implemented, planned, and compensated or how they will be implemented in the future. The table contains: (1) the NIST SP Publication and revision number (2) the security control family and specific control with applicable enhancements; (3) if the security control is a common control, hybrid or system specific (4) the implementation statement; how the security control is being implemented or how it will be implemented (5) the implementation status to determine whether the control is in place, not in place, compensated or not applicable and (6) comments to capture specific notes about the control's implementation. (Note: if not in place, an explanation will need to be provided under this section). Implementation statements of controls identified as common will reference the system and/or SSP that the control is inherited from.

2.1 Security Controls

Organizations employ security controls in federal information systems and the environments in which those systems operate in accordance with FIPS Publication 199, FIPS Publication 200, and NIST Special Publications 800-37 and 800-39. Security categorization of federal information and information systems, as required by FIPS Publication 199, is the first step in the risk management process. Next, organizations select an appropriate set of security controls for their information systems by satisfying the minimum-security requirements set forth in FIPS Publication 200. Appendix D includes three security control baselines that are associated with the designated impact levels of information systems as determined during the security categorization process. After baseline selection, organizations tailor the baselines by: (i) identifying/designating common controls; (ii) applying scoping considerations; (iii) selecting compensating controls, if needed; (iv) assigning control parameter values in selection and assignment statements; (v) supplementing the baseline controls with additional controls and control enhancements from the security control catalog; and (vi) providing additional information for control implementation.

2.1.1Access Control (AC)

2.1.1.1 AC-1 Access Control Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
b. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
c. Procedures to facilitate the implementation of the access control policy and associated access controls; and
d. Reviews and updates the current:
e. Access control policy [Assignment: organization-defined frequency]; and
f. Access control procedures [Assignment: organization-defined frequency].

NIST SP 800-53	Access Control	☐ Common (Fully Inherited Control)
Revision 4	[AC-1]	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.1.2 AC-2 Account Management

The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];
g. Monitors the use of, information system accounts;
h. Notifies account managers:
    1. When accounts are no longer required;
    2. When users are terminated or transferred; and
    3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements [*Assignment: organization-defined frequency*]; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT

The organization employs automated mechanisms to support the management of information system accounts.

(2) ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS

The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].

(3) ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS

The information system automatically disables inactive accounts after [Assignment: organization-defined time period].

(4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].

NIST SP 800-53 Revision 4	Access Controls [AC-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-2(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-2(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-2(3)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-2(4)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.1.3 AC-3 Access Enforcement

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

NIST SP 800-53 Revision 4	Access Control [AC-3]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-3

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.1.4 AC-4 Information Flow Enforcement

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [*Assignment: organization-defined information flow control policies*].

NIST SP 800-53 Revision 4	Access Control [AC-4]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-4

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.1.5 AC-5 Separation of Duties

The organization:

a. Separates [*Assignment: organization-defined duties of individuals*];
b. Documents separation of duties of individuals; and
c. Defines information system access authorizations to support separation of duties.

NIST SP 800-53 Revision 4	**Access Control [AC-5]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: **AC-5** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**		

2.1.1.6 AC-6 Least Privilege

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Control Enhancements:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].

(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.

(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].

(9) LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS

The information system audits the execution of privileged functions.

(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

NIST SP 800-53 Revision 4	Access Controls [AC-6]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-6

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-6(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-6(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-6(5)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-6(9)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-6(10)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.1.7 AC-7 Unsuccessful Logon Attempts

The information system:

a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*]; and
b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next logon prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded.

NIST SP 800-53 Revision 4	Access Control [AC-7]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-7

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.1.8 AC-8 System Use Notification

The information system:

a. Displays to users [*Assignment: organization-defined system use notification message or banner*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
   1. Users are accessing a U.S. Government information system;
   2. Information system usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
   4. Use of the information system indicates consent to monitoring and recording;
b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
c. For publicly accessible systems:
   1. Displays system use information [*Assignment: organization-defined conditions*], before granting further access;
   2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. Includes a description of the authorized uses of the system.

NIST SP 800-53 Revision 4	Access Control [AC-8]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-8

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.1.9 AC-11 Session Lock

The information system:

a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Control Enhancements:

(1) SESSION LOCK | PATTERN-HIDING DISPLAYS

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

NIST SP 800-53 Revision 4	Access Control [AC-11]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-11

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Implementation Statement:

AC-11(1)

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.1.10 AC-12 Session Termination

The information system automatically terminates a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

NIST SP 800-53 Revision 4	Access Control [AC-12]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-12

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.1.11 AC-14 Permitted Actions without Identification or Authentication

The organization:

a. Identifies [*Assignment: organization-defined user actions*] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

NIST SP 800-53 Revision 4	Access Control [AC-14]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-14

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.1.12 AC-17 Remote Access

The organization:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorizes remote access to the information system prior to allowing such connections.

Control Enhancements:

(1) REMOTE ACCESS | AUTOMATED MONITORING / CONTROL

The information system monitors and controls remote access methods.

(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

(3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS

The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points.

(4) REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS

The organization:

(a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and

(b) Documents the rationale for such access in the security plan for the information system.

NIST SP 800-53	Access Control	☐ Common (Fully Inherited Control)
Revision 4	[AC-17]	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-17

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-17(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-17(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-17(3)

Implementation Statement:

Implementation Status: Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**
Control Enhancement AC-17(4) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.1.13 AC-18 Wireless Access

The organization:

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
b. Authorizes wireless access to the information system prior to allowing such connections.

Control Enhancements:

(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION

The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.

NIST SP 800-53 **Revision 4**	**Access Control** **[AC-18]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: **AC-18**		

Implementation Status: Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**
Control Enhancement AC-18(1) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.1.14 AC-19 Access Control for Mobile Devices

The organization:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b. Authorizes the connection of mobile devices to organizational information systems.

(5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION

The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

NIST SP 800-53 Revision 4	Access Control [AC-19]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: **AC-19**		

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-19(5)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.1.15 AC-20 Use of External Information Systems

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a. Access the information system from external information systems; and
b. Process, store, or transmit organization-controlled information using external information systems.

Control Enhancements:

(1) USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

(a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or

(b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

(2) USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES

The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

NIST SP 800-53 Revision 4	Access Control [AC-20]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-20

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-20(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AC-20(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.1.16 AC-21 Information Sharing

The organization:

a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and
b. Employs [*Assignment: organization-defined automated mechanisms or manual processes*] to assist users in making information sharing/collaboration decisions.

NIST SP 800-53 **Revision 4**	**Access Control** **[AC-21]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-21

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.1.17 AC-22 Publicly Accessible Content

The organization:

a. Designates individuals authorized to post information onto a publicly accessible information system;
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
d. Reviews the content on the publicly accessible information system for nonpublic information [*Assignment: organization-defined frequency*] and removes such information, if discovered.

NIST SP 800-53 Revision 4	Access Control [AC-22]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AC-22

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.2Awareness and Training (AT)

2.1.2.1 AT-1 Security Awareness and Training Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
b. Reviews and updates the current:
   1. Security awareness and training policy [*Assignment: organization-defined frequency*]; and
   2. Security awareness and training procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53	Awareness and Training	☐ Common (Fully Inherited Control)

Revision 4	[AT-1]	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AT-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.2.2 AT-2 Security Awareness Training

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;
b. When required by information system changes; and
c. [*Assignment: organization-defined frequency*] thereafter.

Control Enhancements:

(2) SECURITY AWARENESS | INSIDER THREAT

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

NIST SP 800-53 Revision 4	Awareness and Training [AT-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AT-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AT-2(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.2.3 AT-3 Role-Based Security Training

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes; and
c. [*Assignment: organization-defined frequency*] thereafter.

NIST SP 800-53 Revision 4	Awareness and Training [AT-3]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AT-3

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.2.4 AT-4 Security Training Records

The organization:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
b. Retains individual training records for [*Assignment: organization-defined time period*].

NIST SP 800-53	**Awareness and Training**	☐ Common (Fully Inherited Control)
Revision 4	**[AT-4]**	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AT-4

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.3Audit and Accountability (AU)

2.1.3.1 AU-1 Audit and Accountability Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

b. Reviews and updates the current:
   1. Audit and accountability policy [*Assignment: organization-defined frequency*]; and
   2. Audit and accountability procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Audit and Accountability [AU-1]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AU-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.3.2 AU-2 Audit Events

The organization:

a. Determines that the information system is capable of auditing the following events: [*Assignment: organization-defined auditable events*];
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
d. Determines that the following events are to be audited within the information system: [*Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event*].

Control Enhancements:

(3) AUDIT EVENTS | REVIEWS AND UPDATES

The organization reviews and updates the audited events [Assignment: organization-defined frequency].

NIST SP 800-53 Revision 4	Audit and Accountability [AU-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AU-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AU-2(3)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.3.3 AU-3 Content of Audit Records

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Control Enhancements:

(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information].

NIST SP 800-53 Revision 4	Audit and Accountability [AU-3]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AU-3

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AU-3(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.3.4 AU-4 Audit Storage

The organization allocates audit record storage capacity in accordance with [*Assignment: organization-defined audit record storage requirements*].

NIST SP 800-53 Revision 4	Audit and Accountability [AU-4]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AU-4

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.3.5 AU-5 Response to Audit Processing Failures

The information system:

a. Alerts [*Assignment: organization-defined personnel or roles*] in the event of an audit processing failure; and
b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

NIST SP 800-53 Revision 4	Audit and Accountability [AU-5]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AU-5

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.3.6 AU-6 Audit Review, Analysis, and Reporting

The organization:

a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*]; and
b. Reports findings to [*Assignment: organization-defined personnel or roles*].

Control Enhancements:

(1) AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

(3) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

NIST SP 800-53 Revision 4	Audit and Accountability [AU-6]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AU-6

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AU-6(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐

Scoped **Comments:**
Control Enhancement AU-6(3) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.3.7 AU-7 Audit Reduction and Report Generation

The information system provides an audit reduction and report generation capability that:

a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
b. Does not alter the original content or time ordering of audit records.

Control Enhancements:

(1) AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING

The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].

NIST SP 800-53	**Audit and Accountability**	☐ Common (Fully Inherited Control)
Revision 4	**[AU-7]**	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: Does not apply to Low systems according to NIST SP 800-53 Rev 4. **AU-7**		

Implementation Status: Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**
Implementation Statement: **AU-7(1)** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.3.8 AU-8 Time Stamps

The information system:

a. Uses internal system clocks to generate time stamps for audit records; and
b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [*Assignment: organization-defined granularity of time measurement*].

Control Enhancements:

(1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

The information system:

(a) Compares the internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and

(b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].

NIST SP 800-53 **Revision 4**	**Audit and Accountability** **[AU-8]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control)

	☐ System Specific Control

Implementation Statement:

AU-8

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AU-8(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.3.9 AU-9 Protection of Audit Information

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Control Enhancements:

(4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS

The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users].

NIST SP 800-53	**Audit and Accountability**	☐ Common (Fully Inherited Control)

Revision 4	[AU-9]	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

AU-9

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement AU-9(4)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.3.10 AU-11 Audit Record Retention

The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

NIST SP 800-53	Audit and Accountability	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control)
Revision 4	[AU-11]	☐ System Specific Control

Implementation Statement: **AU-11** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.3.11 AU-12 Audit Generation

The information system:

a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [*Assignment: organization-defined information system components*];
b. Allows [*Assignment: organization-defined personnel or roles*] to select which auditable events are to be audited by specific components of the information system; and
c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

NIST SP 800-53 **Revision 4**	**Audit and Accountability** **[AU-12]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: **AU-12** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**		

2.1.4Security Assessment and Authorization (CA)

2.1.4.1 CA-1 Security Assessment and Authorization Policies and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and

b. Reviews and updates the current:
   1. Security assessment and authorization policy [*Assignment: organization-defined frequency*]; and
   2. Security assessment and authorization procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Security Assessment and Authorization [CA-1]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CA-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.4.2 CA-2 Security Assessments

The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:
   1. Security controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine security control effectiveness; and
   3. Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls

are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment to [*Assignment: organization-defined individuals or roles*].

Control Enhancements:

(1) SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS

The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.

NIST SP 800-53 Revision 4	Security Assessment and Authorization [CA-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CA-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CA-2(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.4.3 CA-3 System Interconnections

The organization:

a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Reviews and updates Interconnection Security Agreements [*Assignment: organization-defined frequency*].

Control Enhancements:

(5) SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS

The organization employs [Selection: allow-all, deny-by-exception; deny-all, permit-by-exception] policy for allowing [Assignment: organization-defined information systems] to connect to external information systems.

NIST SP 800-53 Revision 4	Security Assessment and Authorization [CA-3]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CA-3

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CA-3(5)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐

Scoped **Comments:**

2.1.4.4 CA-5 Plan of Action and Milestones

The organization:

a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

NIST SP 800-53 Revision 4	Security Assessment and Authorization [CA-5]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CA-5

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.4.5 CA-6 Security Authorization

The organization:

a. Assigns a senior-level executive or manager as the authorizing official for the information system;
b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
c. Updates the security authorization [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Security Assessment and Authorization [CA-6]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CA-6

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.4.6 CA-7 Continuous Monitoring

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of [*Assignment: organization-defined metrics*] to be monitored;
b. Establishment of [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessments supporting such monitoring;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
e. Correlation and analysis of security-related information generated by assessments and monitoring;
f. Response actions to address results of the analysis of security-related information; and
g. Reporting the security status of organization and the information system to [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*].

Control Enhancements:

(1) CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT

The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.

NIST SP 800-53	Security Assessment and Authorization	☐ Common (Fully Inherited Control)

Revision 4	[CA-7]	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CA-7

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CA-7(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.4.7 CA-9 Internal System Connections

The organization:

a. Authorizes internal connections of [*Assignment: organization-defined information system components or classes of components*] to the information system; and
b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

NIST SP 800-53 Revision 4	Security Assessment and Authorization [CA-9]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CA-9

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.5Configuration Management (CM)

2.1.5.1 CM-1 Configuration Management Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and

b. Reviews and updates the current:
   1. Configuration management policy [*Assignment: organization-defined frequency*]; and
   2. Configuration management procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Configuration Management [CM-1]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CM-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.5.2 CM-2 Baseline Configuration

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Control Enhancements:

(1) BASELINE CONFIGURATION | REVIEWS AND UPDATES

The organization reviews and updates the baseline configuration of the information system:

(a) [Assignment: organization-defined frequency];

(b) When required due to [Assignment organization-defined circumstances]; and

(c) As an integral part of information system component installations and upgrades.

(3) BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS

The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.

(7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS

The organization:

(a) Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and

(b) Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.

NIST SP 800-53	**Configuration Management**	☐ Common (Fully Inherited Control)
Revision 4	**[CM-2]**	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CM-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CM-2(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CM-2(3)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CM-2(7)

Implementation Statement:

Implementation Status: Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.5.3 CM-3 Configuration Change Control

The organization:

a. Determines the types of changes to the information system that are configuration-controlled;
b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
c. Documents configuration change decisions associated with the information system;
d. Implements approved configuration-controlled changes to the information system;
e. Retains records of configuration-controlled changes to the information system for [*Assignment: organization-defined time period*];
f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
g. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board*] that convenes [*Selection (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].

Control Enhancements:

(2) CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

NIST SP 800-53 **Revision 4**	**Configuration Management** **[CM-3]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: Does not apply to Low systems according to NIST SP 800-53 Rev 4. **CM-3** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐		

Scoped **Comments:**
Control Enhancement CM-3(2) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.5.4 CM-4 Security Impact Analysis

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

NIST SP 800-53 **Revision 4**	**Configuration Management** **[CM-4]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: **CM-4** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**		

2.1.5.5 CM-5 Access Restrictions for Change

The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

NIST SP 800-53 Revision 4	Configuration Management [CM-5]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CM-5

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.5.6 CM-6 Configuration Settings

The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

NIST SP 800-53 Revision 4	Configuration Management [CM-6]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CM-6

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.5.7 CM-7 Least Functionality

The organization:

a. Configures the information system to provide only essential capabilities; and
b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services*].

Control Enhancements:

(1) LEAST FUNCTIONALITY | PERIODIC REVIEW

The organization:

(a) Reviews the information system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and

(b) Disables [Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure].

(2) LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION

The information system prevents program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].

(4) LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE / BLACKLISTING

The organization:

(a) Identifies [Assignment: organization-defined software programs not authorized to execute on the information system];

(b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and

(c) Reviews and updates the list of unauthorized software programs [Assignment: organization-defined frequency].

NIST SP 800-53 Revision 4	Configuration Management [CM-7]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CM-7

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CM-7(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CM-7(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CM-7(4)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.5.8 CM-8 Information System Component Inventory

The organization:

a. Develops and documents an inventory of information system components that:
   1. Accurately reflects the current information system;
   2. Includes all components within the authorization boundary of the information system;
   3. Is at the level of granularity deemed necessary for tracking and reporting; and
   4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and
b. Reviews and updates the information system component inventory [*Assignment: organization-defined frequency*].

Control Enhancements:

(1) INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

(3) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

The organization:

(a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and

(b) Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]].

(5) INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

NIST SP 800-53 Revision 4	Configuration Management [CM-8]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CM-8

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CM-8(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CM-8(3)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CM-8(5)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.5.9 CM-9 Configuration Management Plan

The organization develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the information system and places the configuration items under configuration management; and
d. Protects the configuration management plan from unauthorized disclosure and modification.

NIST SP 800-53 Revision 4	Configuration Management [CM-9]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CM-9

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐

Scoped

Comments:

2.1.5.10 CM-10 Software Usage Restrictions

The organization:

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

NIST SP 800-53 Revision 4	Configuration Management [CM-10]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CM-10

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.5.11 CM-11 User-Installed Software

The organization:

a. Establishes [*Assignment: organization-defined policies*] governing the installation of software by users;
b. Enforces software installation policies through [*Assignment: organization-defined methods*]; and

c. Monitors policy compliance at [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Configuration Management [CM-11]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CM-11

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.6Contingency Planning (CP)

2.1.6.1 CP-1 Contingency Planning Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

b. Reviews and updates the current:
   1. Contingency planning policy [*Assignment: organization-defined frequency*]; and
   2. Contingency planning procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Contingency Planning [CP-1]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CP-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.6.2 CP-2 Contingency Plan

The organization:

a. Develops a contingency plan for the information system that:
   1. Identifies essential missions and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
   6. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];
b. Distributes copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*];
e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicates contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*]; and
g. Protects the contingency plan from unauthorized disclosure and modification.

Control Enhancements:

(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS

The organization coordinates contingency plan development with organizational elements responsible for related plans.

(3) CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

The organization plans for the resumption of essential missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.

(8) CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS

The organization identifies critical information system assets supporting essential missions and business functions.

NIST SP 800-53 Revision 4	Contingency Planning [CP-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CP-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CP-2(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CP-2(3)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CP-2(8)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.6.3 CP-3 Contingency Training

The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

a. Within [*Assignment: organization-defined time period*] of assuming a contingency role or responsibility;
b. When required by information system changes; and
c. [*Assignment: organization-defined frequency*] thereafter.

NIST SP 800-53 Revision 4	Contingency Planning [CP-3]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CP-3

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.6.4 CP-4 Contingency Plan Testing

The organization:

a. Tests the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective actions, if needed.

Control Enhancements:

(1) CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS
The organization coordinates contingency plan testing with organizational elements responsible for related plans.

NIST SP 800-53 Revision 4	Contingency Planning [CP-4]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CP-4

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CP-4(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.6.5 CP-6 Alternate Storage Site

The organization:

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Control Enhancements:

(1) ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

.

(3) ALTERNATE STORAGE SITE | ACCESSIBILITY

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

NIST SP 800-53 Revision 4	Contingency Planning [CP-6]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CP-6

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CP-6(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CP-6(3)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.6.6 CP-7 Alternate Processing Site

The organization:

a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined information system operations*] for essential missions/business functions within [*Assignment: organization-defined time period consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable;
b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

Control Enhancements:

(1) ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE

The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

(2) ALTERNATE PROCESSING SITE | ACCESSIBILITY

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

(3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE

The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

NIST SP 800-53 Revision 4	Contingency Planning [CP-7]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CP-7

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement CP-7(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:
Control Enhancement CP-7(2) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**
Control Enhancement CP-7(3) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.6.7 CP-8 Telecommunications Services

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [*Assignment: organization-defined information system operations*] for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Control Enhancements:

(1) TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS

The organization:

(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and

(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

(2) TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

NIST SP 800-53 Revision 4	Contingency Planning [CP-8]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

CP-8

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Implementation Statement:

CP-8(1)

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Implementation Statement:

CP-8(2)

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.6.8 CP-9 Information System Backup

The organization:

a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];
b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];
c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and
d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Control Enhancements:

(1) INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY

The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.

NIST SP 800-53	**Contingency Planning**	☐ Common (Fully Inherited Control)
Revision 4	**[CP-9]**	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement: **CP-9** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**
Control Enhancement CP-9(1) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.6.9 CP-10 Information System Recovery and Reconstitution

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Control Enhancements:

(2) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY

The information system implements transaction recovery for systems that are transaction-based.

NIST SP 800-53	**Contingency Planning**	☐ Common (Fully Inherited Control)
Revision 4	**[CP-10]**	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement: **CP-10** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**
Implementation Statement: **CP-10(2)** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.7Identification and Authentication (IA)

2.1.7.1 IA-1 Identification and Authentication Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
b. Reviews and updates the current:
   1. Identification and authentication policy [*Assignment: organization-defined frequency*]; and
   2. Identification and authentication procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Identification and Authentication [IA-1]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

IA-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.7.2 IA-2 Identification and Authentication

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Control Enhancements:

(1) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS

The information system implements multifactor authentication for network access to privileged accounts.

(2) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS

The information system implements multifactor authentication for network access to non-privileged accounts.

(3) IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS

The information system implements multifactor authentication for local access to privileged accounts.

(8) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

(11) IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].

(12) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

NIST SP 800-53 Revision 4	Identification and Authentication [IA-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

IA-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IA-2(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IA-2(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IA-2(3)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IA-2(8)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IA-2(11)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:
Control Enhancement IA-2(12) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.7.3 IA-3 Device Identification and Authentication

The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.

NIST SP 800-53 **Revision 4**	**Identification and Authentication** **[IA-3]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: **IA-3** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**		

2.1.7.4 IA-4 Identifier Management

The organization manages information system identifiers by:

a. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;
c. Assigning the identifier to the intended individual, group, role, or device;
d. Preventing reuse of identifiers for [*Assignment: organization-defined time period*]; and
e. Disabling the identifier after [*Assignment: organization-defined time period of inactivity*].

NIST SP 800-53 Revision 4	Identification and Authentication [IA-4]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

IA-4

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.7.5 IA-5 Authenticator Management

The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*];
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

j. Changing authenticators for group/role accounts when membership to those accounts changes.

Control Enhancements:

(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION

The information system, for password-based authentication:

a. Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*];

b. Enforces at least the following number of changed characters when new passwords are created: [*Assignment: organization-defined number*];

c. Stores and transmits only encrypted representations of passwords;

d. Enforces password minimum and maximum lifetime restrictions of [*Assignment: organization-defined numbers for lifetime minimum, lifetime maximum*];

e. Prohibits password reuse for [*Assignment: organization-defined number*] generations; and

f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

(2) AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION

The information system, for PKI-based authentication:

a. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;

b. Enforces authorized access to the corresponding private key;

c. Maps the authenticated identity to the account of the individual or group; and

d. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

(3) AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION

The organization requires that the registration process to receive [*Assignment: organization-defined types of and/or specific authenticators*] be conducted [Selection: in person; by a trusted third party] before [*Assignment: organization-defined registration authority*] with authorization by [Assignment: organization-defined personnel or roles].

(11) AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION

The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].

NIST SP 800-53	Identification and Authentication	☐ Common (Fully Inherited Control)

Revision 4	[IA-5]	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

IA-5

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IA-5(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IA-5(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IA-5(3)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IA-5(11)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.7.6 IA-6 Authenticator Feedback

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

NIST SP 800-53 Revision 4	Identification and Authentication [IA-6]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

IA-6

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐

Scoped

Comments:

2.1.7.7 IA-7 Cryptographic Module Authentication

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

NIST SP 800-53 Revision 4	Identification and Authentication [IA-7]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

IA-7

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.7.8 IA-8 Identification and Authentication (Non-Organizational Users)

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Control Enhancements:

(1) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

(2) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF THIRD-PARTY CREDENTIALS

The information system accepts only FICAM-approved third-party credentials.

(3) IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS

The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials.

(4) IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-ISSUED PROFILES

The information system conforms to FICAM-issued profiles.

NIST SP 800-53 Revision 4	Identification and Authentication [IA-8]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

IA-8

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IA-8(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IA-8(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IA-8(3)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IA-8(4)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.8Incident Response (IR)

2.1.8.1 IR-1 Incident Response Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
b. Reviews and updates the current:
   1. Incident response policy [*Assignment: organization-defined frequency*]; and
   2. Incident response procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Incident Response [IR-1]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

IR-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.8.2 IR-2 Incident Response Training

The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

a. Within [*Assignment: organization-defined time period*] of assuming an incident response role or responsibility;
b. When required by information system changes; and
c. [*Assignment: organization-defined frequency*] thereafter.

NIST SP 800-53 Revision 4	Incident Response [IR-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

IR-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.8.3 IR-3 Incident Response Testing

The organization tests the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the incident response effectiveness and documents the results.

Control Enhancements:

(2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

The organization coordinates incident response testing with organizational elements responsible for related plans.

NIST SP 800-53 Revision 4	Incident Response [IR-3]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement: Does not apply to Low systems according to NIST SP 800-53 Rev 4.

IR-3

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:
Control Enhancement IR-3(2) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.8.4 IR-4 Incident Handling

The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinates incident handling activities with contingency planning activities; and
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Control Enhancements:

(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES

The organization employs automated mechanisms to support the incident handling process.

NIST SP 800-53 **Revision 4**	**Incident Response** **[IR-4]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: **IR-4** **Implementation Status:** Status (check all that apply):		

☐ Implemented (In Place)	☐ Planned (Not in Place)	☐ Compensated	☐ Not Applicable	☐ Scoped

Comments:

Control Enhancement IR-4(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place)	☐ Planned (Not in Place)	☐ Compensated	☐ Not Applicable	☐ Scoped

Comments:

2.1.8.5 IR-5 Incident Monitoring

The organization tracks and documents information system security incidents.

NIST SP 800-53 Revision 4	Incident Response [IR-5]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

IR-5

Implementation Status: Status (check all that apply):

☐ Implemented (In Place)	☐ Planned (Not in Place)	☐ Compensated	☐ Not Applicable	☐ Scoped

Comments:

2.1.8.6 IR-6 Incident Reporting

The organization:

a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time period*]; and
b. Reports security incident information to [*Assignment: organization-defined authorities*].

Control Enhancements:

(1) INCIDENT REPORTING | AUTOMATED REPORTING

The organization employs automated mechanisms to assist in the reporting of security incidents.

NIST SP 800-53 Revision 4	Incident Response [IR-6]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

IR-6

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IR-6(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.8.7 IR-7 Incident Response Assistance

The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Control Enhancements:

(1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT

The organization employs automated mechanisms to increase the availability of incident response-related information and support.

NIST SP 800-53 Revision 4	Incident Response [IR-7]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

IR-7

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement IR-7(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.8.8 IR-8 Incident Response Plan

The organization:

a. Develops 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. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
    5. Defines reportable incidents;
    6. Provides metrics for measuring the incident response capability within the organization;
    7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
    8. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];
b. Distributes copies of the incident response plan to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*];
c. Reviews the incident response plan [*Assignment: organization-defined frequency*];
d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
e. Communicates incident response plan changes to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*]; and
f. Protects the incident response plan from unauthorized disclosure and modification.

NIST SP 800-53 Revision 4	Incident Response [IR-8]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

IR-8

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.9Maintenance (MA)

2.1.9.1 MA-1 System Maintenance Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
b. Reviews and updates the current:
   1. System maintenance policy [*Assignment: organization-defined frequency*]; and
   2. System maintenance procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Maintenance [MA-1]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

MA-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.9.2 MA-2 Controlled Maintenance

The organization:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
c. Requires that [*Assignment: organization-defined personnel or roles*] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
f. Includes [*Assignment: organization-defined maintenance-related information*] in organizational maintenance records.

NIST SP 800-53 Revision 4	Maintenance [MA-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

MA-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.9.3 MA-3 Maintenance Tools

The organization approves, controls, and monitors information system maintenance tools.

Control Enhancements:

(1) MAINTENANCE TOOLS | INSPECT TOOLS

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

(2) MAINTENANCE TOOLS | INSPECT MEDIA

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

NIST SP 800-53 Revision 4	Maintenance [MA-3]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control)

[redacted]	☐ System Specific Control
Implementation Statement: **MA-3** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**	
Control Enhancement MA-3(1) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**	

2.1.9.4 MA-4 Nonlocal Maintenance

The organization:

a. Approves and monitors nonlocal maintenance and diagnostic activities;
b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

Maintains records for nonlocal maintenance and diagnostic activities; and terminates session and network connections when nonlocal maintenance is completed.

Control Enhancements:

(2) NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

NIST SP 800-53 Revision 4	Maintenance [MA-4]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

MA-4

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement MA-4(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.9.5 MA-5 Maintenance Personnel

The organization:

a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

NIST SP 800-53 Revision 4	Maintenance [MA-5]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

MA-5

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.9.6 MA-6 Timely Maintenance

The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined information system components*] within [*Assignment: organization-defined time period*] of failure.

NIST SP 800-53 Revision 4	Maintenance [MA-6]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

MA-6

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.10 Media Protection (MP)

2.1.10.1 MP-1 Media Protection Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
b. Reviews and updates the current:
   1. Media protection policy [*Assignment: organization-defined frequency*]; and
   2. Media protection procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Media Protection [MP-1]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

MP-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.10.2 MP-2 Media Access

The organization restricts access to [*Assignment: organization-defined types of digital and/or non-digital media*] to [*Assignment: organization-defined personnel or roles*

NIST SP 800-53 Revision 4	Media Protection [MP-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control)

		☐ System Specific Control

Implementation Statement:

MP-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.10.3 MP-3 Media Marking

The organization:

a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempts [*Assignment: organization-defined types of information system media*] from marking as long as the media remain within [*Assignment: organization-defined controlled areas*].

NIST SP 800-53	Media Protection	☐ Common (Fully Inherited Control)
Revision 4	[MP-3]	☐ Hybrid (Partially Inherited Control)
		☐ System Specific Control

Implementation Statement:

MP-3

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.10.4 MP-4 Media Storage

The organization:

a. Physically controls and securely stores [*Assignment: organization-defined types of digital and/or non-digital media*] within [*Assignment: organization-defined controlled areas*]; and
b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

NIST SP 800-53 Revision 4	Media Protection [MP-4]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

MP-4

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.10.5 MP-5 Media Transport

The organization:

a. Protects and controls [*Assignment: organization-defined types of information system media*] during transport outside of controlled areas using [*Assignment: organization-defined security safeguards*];
b. Maintains accountability for information system media during transport outside of controlled areas;
c. Documents activities associated with the transport of information system media; and
d. Restricts the activities associated with the transport of information system media to authorized personnel.

Control Enhancements:

(4) MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

NIST SP 800-53 Revision 4	Media Protection [MP-5]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

MP-5

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement MA-5(4)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.10.6 MP-6 Media Sanitization

The organization:

a. Sanitizes [*Assignment: organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and
b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

NIST SP 800-53	Media Protection	☐ Common (Fully Inherited Control)

Revision 4	[MP-6]	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

MP-6

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.10.7 MP-7 Media Use

The organization [*Selection: restricts; prohibits*] the use of [*Assignment: organization-defined types of information system media*] on [*Assignment: organization-defined information systems or system components*] using [*Assignment: organization-defined security safeguards*].

Control Enhancements:

(1) MEDIA USE | PROHIBIT USE WITHOUT OWNER

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

NIST SP 800-53 Revision 4	Media Protection [MP-7]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

MP-7

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**
MP-7(1) Control Enhancement **Implementation Statement:** **Implementation Status:** Status (check all that apply ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.11 Physical and Environmental Protection (PE)

2.1.11.1 PE-1 Physical and Environmental Protection Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and

b. Reviews and updates the current:
   1. Physical and environmental protection policy [*Assignment: organization-defined frequency*]; and
   2. Physical and environmental protection procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53	**Physical and Environmental Protection**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control)
Revision 4	**[PE-1]**	☐ System Specific Control

Implementation Statement:

PE-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.11.2 PE-2 Physical Access Authorizations

The organization:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
b. Issues authorization credentials for facility access;
c. Reviews the access list detailing authorized facility access by individuals [*Assignment: organization-defined frequency*]; and
d. Removes individuals from the facility access list when access is no longer required.

NIST SP 800-53 Revision 4	Physical and Environmental Protection [PE-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PE-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.11.3 PE-3 Physical Access Control

The organization:

a. Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] by;
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress/egress to the facility using [*Selection (one or more):* [*Assignment: organization-defined physical access control systems/devices*]; *guards*];
b. Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*];
c. Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and monitoring*];
e. Secures keys, combinations, and other physical access devices;
f. Inventories [*Assignment: organization-defined physical access devices*] every [*Assignment: organization-defined frequency*]; and
g. Changes combinations and keys [*Assignment: organization-defined frequency*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

NIST SP 800-53 Revision 4	Physical and Environmental Protection [PE-3]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PE-3

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.11.4 PE-4 Access Control for Transmission Medium

The organization controls physical access to [*Assignment: organization-defined information system distribution and transmission lines*] within organizational facilities using [*Assignment: organization-defined security safeguards*].

NIST SP 800-53 Revision 4	Physical and Environmental Protection [PE-4]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PE-4

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.11.5 PE-5 Access Control for Output Devices

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

NIST SP 800-53 Revision 4	Physical and Environmental Protection [PE-5]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PE-5

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.11.6 PE-6 Monitoring Physical Access

The organization:

a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Reviews physical access logs [*Assignment: organization-defined frequency*] and upon occurrence of [*Assignment: organization-defined events or potential indications of events*]; and
c. Coordinates results of reviews and investigations with the organizational incident response capability.

Control Enhancements:

(1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT

The organization monitors physical intrusion alarms and surveillance equipment.

NIST SP 800-53 Revision 4	Physical and Environmental Protection [PE-6]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PE-6

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement PE-6(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.11.7 PE-8 Visitor Access Records

The organization:

a. Maintains visitor access records to the facility where the information system resides for [*Assignment: organization-defined time period*]; and
b. Reviews visitor access records [*Assignment: organization-defined frequency*].

NIST SP 800-53 **Revision 4**	**Physical and Environmental Protection** **[PE-8]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: **PE-8** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**		

2.1.11.8 PE-9 Power Equipment and Cabling

The organization protects power equipment and power cabling for the information system from damage and destruction.

NIST SP 800-53 **Revision 4**	**Physical and Environmental Protection** **[PE-9]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PE-9

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.11.9 PE-10 Emergency Shutoff

The organization:

a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and
c. Protects emergency power shutoff capability from unauthorized activation.

NIST SP 800-53 Revision 4	Physical and Environmental Protection [PE-10]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PE-10

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.11.10 PE-11 Emergency Power

The organization provides a short-term uninterruptible power supply to facilitate [*Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power*] in the event of a primary power source loss.

NIST SP 800-53 Revision 4	Physical and Environmental Protection [PE-11]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PE-11

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.11.11 PE-12 Emergency Lighting

The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

NIST SP 800-53 Revision 4	Physical and Environmental Protection [PE-12]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PE-12

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.11.12 PE-13 Fire Protection

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Control Enhancements:

(3) FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

NIST SP 800-53 Revision 4	Physical and Environmental Protection [PE-13]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PE-13

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:
Control Enhancement PE-13(3) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.11.13 PE-14 Temperature and Humidity Controls

The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and
b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Physical and Environmental Protection [PE-14]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: **PE-14** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped		

Comments:

2.1.11.14 PE-15 Water Damage Protection

The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

NIST SP 800-53 **Revision 4**	**Physical and Environmental Protection** **[PE-15]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PE-15

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.11.15 PE-16 Delivery and Removal

The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.

NIST SP 800-53	**Physical and Environmental**	☐ Common (Fully Inherited Control)

	Protection	☐ Hybrid (Partially Inherited Control)
Revision 4	**[PE-16]**	☐ System Specific Control

Implementation Statement:

PE-16

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.11.16 PE-17 Alternate Work Site

The organization:

a. Employs [*Assignment: organization-defined security controls*] at alternate work sites;
b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

NIST SP 800-53	**Physical and Environmental Protection**	☐ Common (Fully Inherited Control)
		☐ Hybrid (Partially Inherited Control)
Revision 4	**[PE-17]**	☐ System Specific Control

Implementation Statement:

PE-17

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.12 Planning (PL)

2.1.12.1 PL-1 Security Planning Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and

b. Reviews and updates the current:
   1. Security planning policy [*Assignment: organization-defined frequency*]; and
   2. Security planning procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Planning [PL-1]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PL-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.12.2 PL-2 System Security Plan

The organization:

a. Develops a security plan for the information system that:
   1. Is consistent with the organization's enterprise architecture;
   2. Explicitly defines the authorization boundary for the system;
   3. Describes the operational context of the information system in terms of missions and business processes;
   4. Provides the security categorization of the information system including supporting rationale;
   5. Describes the operational environment for the information system and relationships with or connections to other information systems;
   6. Provides an overview of the security requirements for the system;
   7. Identifies any relevant overlays, if applicable;
   8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
   9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
b. Distributes copies of the security plan and communicates subsequent changes to the plan to [*Assignment: organization-defined personnel or roles*];
c. Reviews the security plan for the information system [*Assignment: organization-defined frequency*];
d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
e. Protects the security plan from unauthorized disclosure and modification.

Control Enhancements:

(1)SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES
The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.

NIST SP 800-53 Revision 4	Planning [PL-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PL-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐

Scoped **Comments:**
Control Enhancement PL-2(1) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.12.3 PL-4 Rules of Behavior

The organization:

a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
c. Reviews and updates the rules of behavior [*Assignment: organization-defined frequency*]; and
d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

Control Enhancements:

(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

NIST SP 800-53	**Planning**	☐ Common (Fully Inherited Control)
Revision 4	**[PL-4]**	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PL-4

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement PL-4(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.12.4 PL-8 Information Security Architecture

The organization:

a. Develops an information security architecture for the information system that:
   1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
   2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
   3. Describes any information security assumptions about, and dependencies on, external services;
b. Reviews and updates the information security architecture [*Assignment: organization-defined frequency*] to reflect updates in the enterprise architecture; and
c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

NIST SP 800-53	Planning	☐ Common (Fully Inherited Control)

Revision 4	[PL-8]	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement: Does not apply to Low systems according to NIST SP 800-53 Rev 4.

PL-8

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.13 Personnel Security (PS)

2.1.13.1 PS-1 Personnel Security Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and

b. Reviews and updates the current:
   1. Personnel security policy [*Assignment: organization-defined frequency*]; and
   2. Personnel security procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53	Personnel Security	☐ Common (Fully Inherited Control)
Revision 4	[PS-1]	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PS-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.13.2 PS-2 Position Risk Designation

The organization:

a. Assigns a risk designation to all organizational positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and updates position risk designations [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Personnel Security [PS-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PS-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.13.3 PS-3 Personnel Screening

The organization:

a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals according to [*Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening*].

NIST SP 800-53 Revision 4	Personnel Security [PS-3]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PS-3

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.13.4 PS-4 Personnel Termination

The organization, upon termination of individual employment:

a. Disables information system access within [*Assignment: organization-defined time period*];
b. Terminates/revokes any authenticators/credentials associated with the individual;
c. Conducts exit interviews that include a discussion of [*Assignment: organization-defined information security topics*];
d. Retrieves all security-related organizational information system-related property;
e. Retains access to organizational information and information systems formerly controlled by terminated individual; and
f. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*].

NIST SP 800-53 Revision 4	Personnel Security [PS-4]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PS-4

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐

Scoped

Comments:

2.1.13.5 PS-5 Personnel Transfer

The organization:

a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*];
c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*].

NIST SP 800-53 Revision 4	Personnel Security [PS-5]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PS-5

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.13.6 PS-6 Access Agreements

The organization:

a. Develops and documents access agreements for organizational information systems;

b. Reviews and updates the access agreements [*Assignment: organization-defined frequency*]; and
c. Ensures that individuals requiring access to organizational information and information systems:
   1. Sign appropriate access agreements prior to being granted access; and
   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Personnel Security [PS-6]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: **PS-6** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**		

2.1.13.7 PS-7 Third-Party Personnel Security

The organization:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
c. Documents personnel security requirements;
d. Requires third-party providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [*Assignment: organization-defined time period*]; and
e. Monitors provider compliance.

NIST SP 800-53 Revision 4	Personnel Security [PS-7]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PS-7

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.13.8 PS-8 Personnel Sanctions

The organization:

a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
b. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

NIST SP 800-53 Revision 4	Personnel Security [PS-8]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

PS-8

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.14 Risk Assessment (RA)

2.1.14.1 RA-1 Risk Assessment Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
b. Reviews and updates the current:
   1. Risk assessment policy [*Assignment: organization-defined frequency*]; and
   2. Risk assessment procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	Risk Assessment [RA-1]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

RA-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.14.2 RA-2 Security Categorization

The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

NIST SP 800-53	Risk Assessment	☐ Common (Fully Inherited Control)

Revision 4	[RA-2]	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

RA-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.14.3 RA-3 Risk Assessment

The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]];
c. Reviews risk assessment results [*Assignment: organization-defined frequency*];
d. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and
e. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

NIST SP 800-53 Revision 4	Risk Assessment [RA-3]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

RA-3

Implementation Status: Status (check all that apply):

☐ Implemented (In Place)	☐ Planned (Not in Place)	☐ Compensated	☐ Not Applicable	☐ Scoped

Comments:

2.1.14.4 RA-5 Vulnerability Scanning

The organization:

a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Control Enhancements:

(1) VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY

The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

(2) VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED

The organization updates the information system vulnerabilities scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].

(5) VULNERABILITY SCANNING | PRIVILEGED ACCESS

The information system implements privileged access authorization to [Assignment: organization-identified information system components] for selected [Assignment: organization-defined vulnerability scanning activities].

NIST SP 800-53 Revision 4	Personnel Security [RA-5]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

RA-5

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement RA-5(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement RA-5(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement RA-5(5)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.15 System and Services Acquisition

2.1.15.1 SA-1 System and Services Acquisition Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and

b. Reviews and updates the current:
   1. System and services acquisition policy [*Assignment: organization-defined frequency*]; and
   2. System and services acquisition procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	System and Services Acquisition [SA-1]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SA-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐

Scoped

Comments:

2.1.15.2 SA-2 Allocation of Resources

The organization:

a. Determines information security requirements for the information system or information system service in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

NIST SP 800-53 Revision 4	System and Services Acquisition [SA-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SA-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.15.3 SA-3 System Development Life Cycle

The organization:

a. Manages the information system using [*Assignment: organization-defined system development life cycle*] that incorporates information security considerations;
b. Defines and documents information security roles and responsibilities throughout the system development life cycle;

c. Identifies individuals having information security roles and responsibilities; and
d. Integrates the organizational information security risk management process into system development life cycle activities.

NIST SP 800-53 Revision 4	System and Services Acquisition [SA-3]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SA-3

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.15.4 SA-4 Acquisition Process

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Requirements for protecting security-related documentation;
f. Description of the information system development environment and environment in which the system is intended to operate; and
g. Acceptance criteria.

Control Enhancements:

(1) ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

(2) ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail].

(9) ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

(10) ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

NIST SP 800-53 Revision 4	System and Services Acquisition [SA-4]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SA-4

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SA-4(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐

Scoped

Comments:

Control Enhancement SA-4(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SA-4(9)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SA-4(10)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.15.5 SA-5 Information System Documentation

The organization:

a. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
b. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;
c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [*Assignment: organization-defined actions*] in response;
d. Protects documentation as required, in accordance with the risk management strategy; and
e. Distributes documentation to [*Assignment: organization-defined personnel or roles*].

NIST SP 800-53 Revision 4	System and Services Acquisition [SA-5]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SA-5

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.15.6 SA-8 Security Engineering Principles

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

NIST SP 800-53 Revision 4	System and Services Acquisition [SA-8]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement: Does not apply to Low systems according to NIST SP 800-53 Rev 4.

SA-8

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.15.7 SA-9 External Information System Services

The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ [*Assignment: organization-defined security controls*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Employs [*Assignment: organization-defined processes, methods, and techniques*] to monitor security control compliance by external service providers on an ongoing basis.

Control Enhancements:

(2) EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES

The organization requires providers of [Assignment: organization-defined external information system services] to identify the functions, ports, protocols, and other services required for the use of such services.

NIST SP 800-53 Revision 4	System and Services Acquisition [SA-9]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control)

	☐ System Specific Control

Implementation Statement:

SA-9

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SA-9(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.15.8 SA-10 Developer Configuration Management

The organization requires the developer of the information system, system component, or information system service to:

a. Perform configuration management during system, component, or service [*Selection (one or more): design; development; implementation; operation*];
b. Document, manage, and control the integrity of changes to [*Assignment: organization-defined configuration items under configuration management*];
c. Implement only organization-approved changes to the system, component, or service;
d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
e. Track security flaws and flaw resolution within the system, component, or service and report findings to [*Assignment: organization-defined personnel*].

NIST SP 800-53	**System and Services Acquisition**	☐ Common (Fully Inherited Control)

Revision 4	[SA-10]	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement: Does not apply to Low systems according to NIST SP 800-53 Rev 4.

SA-10

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.15.9 SA-11 Developer Security Testing and Evaluation

The organization requires the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan;
b. Perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation at [*Assignment: organization-defined depth and coverage*];
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during security testing/evaluation.

NIST SP 800-53 Revision 4	System and Services Acquisition [SA-11]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement: Does not apply to Low systems according to NIST SP 800-53 Rev 4.

SA-11

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16 System and Communications Protection

2.1.16.1 SC-1 System and Communications Protection Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. Reviews and updates the current:
   1. System and communications protection policy [*Assignment: organization-defined frequency*]; and
   2. System and communications protection procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	System and Communications [SC-1]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.2 SC-2 Application Partitioning

The information system separates user functionality (including user interface services) from information system management functionality.

NIST SP 800-53 Revision 4	System and Communications [SC-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement: Does not apply to Low systems according to NIST SP 800-53 Rev 4.

SC-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.3 SC-4 Information in Shared Resources

The information system prevents unauthorized and unintended information transfer via shared system resources.

NIST SP 800-53 Revision 4	System and Communications [SC-3]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-4

Implementation Status: Status (check all that apply):

☐ Implemented (In Place)	☐ Planned (Not in Place)	☐ Compensated	☐ Not Applicable	☐ Scoped

Comments:

2.1.16.4 SC-5 Denial of Service Protection

The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined types of denial of service attacks or reference to source for such information*] by employing [*Assignment: organization-defined security safeguards*].

NIST SP 800-53	**System and Communications**	☐ Common (Fully Inherited Control)
Revision 4	**[SC-5]**	☐ Hybrid (Partially Inherited Control)
		☐ System Specific Control

Implementation Statement:

SC-5

Implementation Status: Status (check all that apply):

☐ Implemented (In Place)	☐ Planned (Not in Place)	☐ Compensated	☐ Not Applicable	☐ Scoped

Comments:

2.1.16.5 SC-7 Boundary Protection

The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
b. Implements subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and

c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

Control Enhancements:

(3) BOUNDARY PROTECTION | ACCESS POINTS

The organization limits the number of external network connections to the information system.

Supplemental Guidance: Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections.

(4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES

The organization:

(a) Implements a managed interface for each external telecommunication service;

(b) Establishes a traffic flow policy for each managed interface;

(c) Protects the confidentiality and integrity of the information being transmitted across each interface;

(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and

(e) Reviews exceptions to the traffic flow policy [*Assignment: organization-defined frequency*] and removes exceptions that are no longer supported by an explicit mission/business need.

(5) BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION

The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

(7) BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

NIST SP 800-53	**System and Communications**	☐ Common (Fully Inherited Control)
Revision 4	**[SC-7]**	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-7

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SC-7(3)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SC-7(4)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SC-7(5)

Implementation Statement:

Implementation Status: Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**
Control Enhancement SC-7(7) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.16.6 SC-8 Transmission Confidentiality and Integrity

The information system protects the [*Selection (one or more): confidentiality; integrity*] of transmitted information.

Control Enhancements:

(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION

The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards].

NIST SP 800-53	**System and Communications**	☐ Common (Fully Inherited Control)
Revision 4	**[SC-8]**	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-8

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SC-8(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.7 SC-10 Network Disconnect

The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.

NIST SP 800-53	**System and Communications**	☐ Common (Fully Inherited Control)
Revision 4	**[SC-10]**	☐ Hybrid (Partially Inherited Control)
		☐ System Specific Control

Implementation Statement:

SC-10

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.8 SC-12 Cryptographic Key Establishment and Management

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

NIST SP 800-53 Revision 4	System and Communications [SC-12]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-12

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.9 SC-13 Cryptographic Protection

The information system implements [*Assignment: organization-defined cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

NIST SP 800-53 Revision 4	System and Communications [SC-13]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-13

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.10 SC-15 Collaborative Computing Devices

The information system:

a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and
b. Provides an explicit indication of use to users physically present at the devices.

NIST SP 800-53 Revision 4	System and Communications [SC-15]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-15

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.11 SC-17 Public Key Infrastructure Certificates

The organization issues public key certificates under an [*Assignment: organization-defined certificate policy*] or obtains public key certificates from an approved service provider

NIST SP 800-53 Revision 4	System and Communications [SC-17]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-17

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.12 SC-18 Mobile Code

The organization:

a. Defines acceptable and inacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

NIST SP 800-53	System and Communications	☐ Common (Fully Inherited Control)

Revision 4	[SC-18]	☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-18

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.13 SC-19 Voice Over Internet Protocol

The organization:

a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
b. Authorizes, monitors, and controls the use of VoIP within the information system.

NIST SP 800-53 Revision 4	System and Communications [SC-19]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-19

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.14 SC-20 Secure Name / Address Resolution Service (Authoritative Source)

The information system:

a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

NIST SP 800-53 Revision 4	System and Communications [SC-20]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-20

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.15 SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver)

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

NIST SP 800-53 Revision 4	System and Communications [SC-21]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-21

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.16 SC-22 Architecture and Provisioning for Name / Address Resolution Service

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation

NIST SP 800-53 Revision 4	System and Communications [SC-22]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-22

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.17 SC-23 Session Authenticity

The information system protects the authenticity of communications sessions.

NIST SP 800-53 **Revision 4**	**System and Communications** **[SC-23]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: **SC-23** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**		

2.1.16.18 SC-28 Protection of Information at Rest

The information system protects the [*Selection (one or more): confidentiality; integrity*] of [*Assignment: organization-defined information at rest*].

NIST SP 800-53 **Revision 4**	**System and Communications** **[SC-28]**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-28

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.16.19 SC-39 Process Isolation

The information system maintains a separate execution domain for each executing process.

NIST SP 800-53 Revision 4	System and Communications [SC-39]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SC-39

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.17 System and Information Integrity

2.1.17.1 SI-1 System and Information Integrity Policy and Procedures

The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
b. Reviews and updates the current:
   1. System and information integrity policy [*Assignment: organization-defined frequency*]; and
   2. System and information integrity procedures [*Assignment: organization-defined frequency*].

NIST SP 800-53 Revision 4	System and Information Integrity [SI-1]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SI-1

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.17.2 SI-2 Flaw Remediation

The organization:

a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and
d. Incorporates flaw remediation into the organizational configuration management process.

Control Enhancements:

(2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS

The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation.

NIST SP 800-53 Revision 4	System and Information Integrity [SI-2]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SI-2

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SI-2(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.17.3 SI-3 Malicious Code Protection

The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

c. Configures malicious code protection mechanisms to:
   1. Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources at [*Selection (one or more); endpoint; network entry/exit points*] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
   2. [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and

d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Control Enhancements:

(1) MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT

The organization centrally manages malicious code protection mechanisms.

(2) MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES

The information system automatically updates malicious code protection mechanisms.

NIST SP 800-53 Revision 4	System and Information Integrity [SI-3]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Implementation Statement: **SI-3** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**		
Control Enhancement SI-3(1) **Implementation Statement:**		

Implementation Status: Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**
Control Enhancement SI-3(2) **Implementation Statement:** **Implementation Status:** Status (check all that apply): ☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped **Comments:**

2.1.17.4 SI-4 Information System Monitoring

The organization:

a. Monitors the information system to detect:
    1. Attacks and indicators of potential attacks in accordance with [*Assignment: organization-defined monitoring objectives*]; and
    2. Unauthorized local, network, and remote connections;
b. Identifies unauthorized use of the information system through [*Assignment: organization-defined techniques and methods*];
c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
g. Provides [*Assignment: organization-defined information system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed;* [*Assignment: organization-defined frequency*]].

Control Enhancements:

(2) INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS

The organization employs automated tools to support near real-time analysis of events.

(4) INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions.

(5) INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS

The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].

NIST SP 800-53 Revision 4	System and Information Integrity [SI-4]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SI-4

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SI-4(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SI-4(4)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SI-4(5)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.17.5 SI-5 Security Alerts, Advisories, and Directives

The organization:

a. Receives information system security alerts, advisories, and directives from [*Assignment: organization-defined external organizations*] on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to: [*Selection (one or more):* [*Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined elements within the organization*]; [*Assignment: organization-defined external organizations*]]; and
d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

NIST SP 800-53	**System and Information Integrity**	☐ Common (Fully Inherited Control)
Revision 4	**[SI-5]**	☐ Hybrid (Partially Inherited Control)
		☐ System Specific Control

Implementation Statement:

SI-5

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.17.6 SI-7 Software, Firmware, and Information Integrity

The organization employs integrity verification tools to detect unauthorized changes to [*Assignment: organization-defined software, firmware, and information*].

Control Enhancements:

(1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS

The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].

(7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE

The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.

NIST SP 800-53	**System and Information Integrity**	☐ Common (Fully Inherited Control)
Revision 4	**[SI-7]**	☐ Hybrid (Partially Inherited Control)
		☐ System Specific Control

Implementation Statement: Does not apply to Low systems according to NIST SP 800-53 Rev 4.

SI-7

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SI-7(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SI-7(7)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.17.7 SI-8 Spam Protection

The organization:

a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Control Enhancements:

(1) SPAM PROTECTION | CENTRAL MANAGEMENT

The organization centrally manages spam protection mechanisms.

(2) SPAM PROTECTION | AUTOMATIC UPDATES

The information system automatically updates spam protection mechanisms.

NIST SP 800-53 Revision 4	System and Information Integrity [SI-8]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SI-8

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SI-8(1)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

Control Enhancement SI-8(2)

Implementation Statement:

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.17.8 SI-10 Information Input Validation

The information system checks the validity of [*Assignment: organization-defined information inputs*].

NIST SP 800-53 Revision 4	System and Information Integrity [SI-10]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement: Does not apply to Low systems according to NIST SP 800-53 Rev 4.

SI-10

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.17.9 SI-11 Error Handling

The information system:

a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
b. Reveals error messages only to [*Assignment: organization-defined personnel or roles*].

NIST SP 800-53 Revision 4	System and Information Integrity [SI-11]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SI-11

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

2.1.17.10 SI-12 Information Handling and Retention

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

NIST SP 800-53 Revision 4	System and Information Integrity [SI-12]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement:

SI-12

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐

Scoped **Comments:**

2.1.17.11 SI-16 Memory Protection

The information system implements [*Assignment: organization-defined security safeguards*] to protect its memory from unauthorized code execution.

NIST SP 800-53 Revision 4	System and Information Integrity [SI-16]	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control

Implementation Statement: Does not apply to Low systems according to NIST SP 800-53 Rev 4.

SI-16

Implementation Status: Status (check all that apply):

☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable ☐ Scoped

Comments:

3 APPENDIX LISTING

3.1 Required Appendices

APPENDIX	DESCRIPTION	STATUS
A	Acronym List	Refer to Appendix 3.2 below
B	Definitions	Refer to Appendix 3.3 below
C	Applicable Laws and References	Refer to Appendix 3.4 below
D	Agency IT Master Inventory	System Security Plan Appendices.doc
E	Security Assessment Report Matrix	SecurityAssessmentReport.pdf
G	System Documentation	[ENTER NAME OF SSP]
H	System Rules of Behavior	System Security Plan Appendices.doc
I	Security Awareness and Training Plan	System Security Plan Appendices.doc
J	Incident Response Plan	System Security Plan Appendices.doc
K	Configuration Management Plan	System Security Plan Appendices.doc

3.2 System Specific Appendices

APPENDIX	DESCRIPTION	STATUS
E2	Prior Security Assessment Report Matrix	[System Name] SAR Matrix.doc

3.3 Acronym List

TERM	DEFINITION
AO	Authorizing Official
ASSERT	Automated Security Self-Evaluation and Remediation Tracking
ATO	Authorization to Operate
BSM	Boundary Scope Memo
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CONOPS	Concept of Operations
COTS	Commercial off the Shelf
CSAM	Cyber Security and Asset Management
CSO	Component Security Officer
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard(s)
FISMA	Federal Information Security Management Act
GMT	Greenwich Mean Time
HW	Hardware
ISA	Interconnection Security Agreement
ISSH	Information System Security Handbook
IT	Information Technology
MD	Maryland
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NCC	National Coordinating Center for Communications
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIS	Office of Information Security
OMB	Office of Management and Budget
OS	Operating System
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
POC	Point of Contact

TERM	DEFINITION
PRIDE	Project Resource Guide
PSC	Program Support Center
RBD	Risk-Based Decision
SAM	Security Authorization Manager
SAR	Security Assessment Report
SBU	Sensitive But Unclassified
SDLC	Systems Development Life Cycle
SDLCM	Systems Development Life Cycle Methodology
SME	Subject Matter Expert
SO	System Owner
SP	Special Publication
SPM	System Project Manager
SRA	Security Risk Assessment
SSA	Social Security Administration
SSC	Secure Standards Council
SSP	System Security Plan
SW	Software
TIC	Trusted Internet Connection
TSL	Transport Layer Security
U.S.C.	United States Code
UTC	Coordinated Universal Time
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

3.4 Definitions/Glossary

Term	Definition
Accreditation	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Accreditation Boundary	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected.
Accreditation Package	The evidence provided to the authorizing official to be used in the security accreditation decision process. Evidence includes, but is not limited to: (i) the system security plan; (ii) the assessment results from the security certification; and (iii) the plan of action and milestones.
Assessment Procedure	A set of activities or actions employed by an assessor to determine the extent to which a security control is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Automated Information System (AIS)	An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.
Certification	The comprehensive evaluation of the technical and non-technical security features of an AIS and other safeguards, made in support of the accreditation process that establishes the extent to which a particular design and implementation meet a specified set of security requirements.
Common Security Control	Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the C&A processes of an agency information system where that control has been applied.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation. [CNSS Inst. 4009]

Term	Definition
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. [OMB Circular A-130, Appendix III]
Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. [CNSS Inst. 4009]
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., Sec. 3542]
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information. [CNSS Inst. 4009]
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III]
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation. [FIPS 199]
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]
Major Application	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. [OMB Circular A-130, Appendix III]
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. [NIST SP 800-18]
Minor Application	An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems). [NIST SP 800-18]
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. [OMB Memorandum M-02-09]

Term	Definition
Risk	The level of impact on agency operations, (including mission, functions, image, or reputation), agency assets, or individuals, resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [NIST SP 800-30]
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses. [NIST SP 800-30]
Risk Management	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations. [NIST SP 800-30]
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. [FIPS 199]
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [FIPS 199]
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. [NIST SP 800-18]
System-specific Security Control	A security control for an information system that has not been designated as a common security control.
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. [NIST SP 800-18]
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [CNSS Inst. 4009, Adapted]

Term	Definition
User	Person or process accessing an AIS either by direct connections (e.g., via terminals), or indirect connections (e.g., prepare input data or receive output that is not reviewed for content or classification by a responsible individual).
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [CNSS Inst. 4009, Adapted]
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system. [CNSS Inst. 4009]

3.5 Applicable Laws and References

Applicable Laws or Regulations Affecting the System
Federal Policies/Directives/Guidance
Committee on National Security Systems (CNSS) Instruction 4009, National Information Assurance Glossary, June 2006
Committee on National Security Systems (CNSS) Instruction 1253, Security Categorization and Control Selection for National Security Systems, October 2009
Freedom of Information Act (FOIA)
Federal Information Security Management Act (FISMA) of 2002
Federal Information Security Modernization Act (FISMA) of 2014
Federal Managers' Financial Integrity Act (FMFIA)
Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
Homeland Security Presidential Directive (HSPD)-7, Critical Infrastructure Identification, Prioritization, and Protection
Homeland Security Presidential Directive/HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors
Homeland Security Presidential Directive/HSPD-20, National Continuity Policy
National Archives & Records Administration (NARA)
National Institute of Standards and Technology (NIST) Special Publications (SP) 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, February 2006
NIST SP 800-27, Revision A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2004
NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments, September 2012
NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems, May 2010
NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010
NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011
NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, October 2003
NIST SP 800-52, Guidelines for Selecting and Use of Transport Layer Security (TSL) Implementations, April 2014
NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
NIST SP 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information

Applicable Laws or Regulations Affecting the System
Systems and Organizations: Building Effective Assessment Plans, December 2014
NIST SP 800-59, Guideline for Identifying an Information System as a National Security System, August 2003.
NIST SP 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.
NIST SP 800-64, Rev 2, Security Consideration in the Information System Development Life Cycle, October 2008
NIST SP 800-70, Revision 3, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers, March 2015
NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010
NIST SP 800-126, Revision 1, The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2, February 2011.
Office of Management and Budget (OMB) Circular A-123 Management Accountability and Control, 1995
OMB Circular A-127 Financial Management Systems, 1993
OMB Circular A-130 Management of Federal Information Resources, 2000
NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011
NIST SP 800-145, The NIST Definition of Cloud Computing, September 2011
NIST SP 800-146, Cloud Computing Synopsis and Recommendations, May 2012
OMB Circular M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, October 2001.
Paperwork Reduction Act, May 1995
Privacy Act of 1974, as amended
Social Security Act of 2013
SSA Departmental Guidance
ISSH, Information System Security Handbook - http://eis.ba.ssa.gov/ssasso/issh/tableofcontents.htm
OIS Guidance, http://ois.ssahost.ba.ssa.gov/dspp/fisma/security_assessment_authorization.htm
PRIDE, http://pride.ssahost.ba.ssa.gov/
CSAM, https://csamssa.justapps.doj.gov/CSAM/login.aspx?ReturnUrl=%2fCSAM%2fDefault.aspx
ISAHB, Information Security Authorization Handbook (dated June 2014)

Appendix A. <Appendix Name>Appendix body

✍ **NOTE**: Automatic section numbering (Heading 1, Heading 2, etc.) should not be applied to the appendix body. The numbering will be a continuation of the numbering from the body of the document, and will not accurately reflect the appendix location.

Appendix B. Acronym List

✍ Make sure all acronyms within this document are included in the acronym list. Delete any that are not used.

Acronym	Definition
AO	Authorizing Official
APM	Application Portfolio Management
APP	Application
BRM	Business Reference Model
BSM	Boundary Scope Memorandum
CSAM	Cybersecurity Assessment and Management
CSO	Component Security Officer
DB	Database
DBMS	Database Management System
DCS	Deputy Commissioner for Systems
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FOUO	For Official Use Only
FTP	File Transfer Protocol
HW	Hardware
ID	Identification
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
IT	Information Technology
IV&V	Independent Verification and Validation
L2TP	Layer 2 Tunneling Protocol
MA	Major Application
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NCC	National Computer Center
NIST	National Institute of Standards and Technology
NMS	Network Management System
OIS	Office of Information Security
OS	Operating System
PDA	Personal Digital Assistant

Acronym	Definition
SAM	Security Authorization Manager
SBU	Sensitive But Unclassified
SCQ	Significant Change Questionnaire
SO	System Owner
SP	Special Publication
SSA	Social Security Administration
SSC	Secondary Support Center
SSP	System Security Plan
V-HW	Virtual Hardware
VPN	Virtual Private Network

EXHIBIT F

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 G

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	Name	Month/Year	Month/Year
#1		To	#3		To
#2		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.

Month/Year Month/Year **#1** To Present	Street Address		Apt. #	City (Country)			State	ZIP Code
Name of Person Who Knows You	Street Address	Apt. #	City (Country)		State	ZIP Code	Telephone Number ( )	
Month/Year Month/Year **#2** To	Street Address		Apt. #	City (Country)			State	ZIP Code
Name of Person Who Knew You	Street Address	Apt. #	City (Country)		State	ZIP Code	Telephone Number ( )	
Month/Year Month/Year **#3** To	Street Address		Apt. #	City (Country)			State	ZIP Code
Name of Person Who Knew You	Street Address	Apt. #	City (Country)		State	ZIP Code	Telephone Number ( )	
Month/Year Month/Year **#4** To	Street Address		Apt. #	City (Country)			State	ZIP Code
Name of Person Who Knew You	Street Address	Apt. #	City (Country)		State	ZIP Code	Telephone Number ( )	
Month/Year Month/Year **#5** To	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.

Month/Year Month/Year **#1** To	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 ( )	
Month/Year Month/Year **#2** To	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 ( )	
Month/Year Month/Year **#3** To	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.

#1 Month/Year To Present	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 #1)*	Month/Year To	Month/Year	Position Title		Supervisor	
	Month/Year To	Month/Year	Position Title		Supervisor	
	Month/Year To	Month/Year	Position Title		Supervisor	

#2 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 #2)*	Month/Year To	Month/Year	Position Title		Supervisor	
	Month/Year To	Month/Year	Position Title		Supervisor	
	Month/Year To	Month/Year	Position Title		Supervisor	

#3 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 #3)*	Month/Year To	Month/Year	Position Title		Supervisor	
	Month/Year To	Month/Year	Position Title		Supervisor	
	Month/Year To	Month/Year	Position Title		Supervisor	

Enter your Social Security Number before going to the next page →

YOUR EMPLOYMENT ACTIVITIES *(CONTINUED)*

Month/Year To	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
#4			

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 ( )

	Month/Year To	Month/Year To	Position Title	Supervisor
PREVIOUS PERIODS OF ACTIVITY *(Block #4)*				

Month/Year To	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
#5			

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 ( )

	Month/Year To	Month/Year To	Position Title	Supervisor
PREVIOUS PERIODS OF ACTIVITY *(Block #5)*				

Month/Year To	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank
#6			

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 ( )

	Month/Year To	Month/Year To	Position Title	Supervisor
PREVIOUS PERIODS OF ACTIVITY *(Block #6)*				

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)*
- ☐ **2** - Married
- ☐ **3** - Separated
- ☐ **4** - Legally Separated
- ☐ **5** - Divorced
- ☐ **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	Month/Year	Code	Service/Certificate No.	O	E	Status				Country
						Active	Active Reserve	Inactive Reserve	National Guard *(State)*	
	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	Month/Year	Code	Country		Month/Year	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 Month/Year To	Controlled Substance/Prescription Drug Used	Number of Times Used
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 H

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

ORI

RESIDENCE OF PERSON FINGERPRINTED

DATE OF BIRTH Month Day Year DOB

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

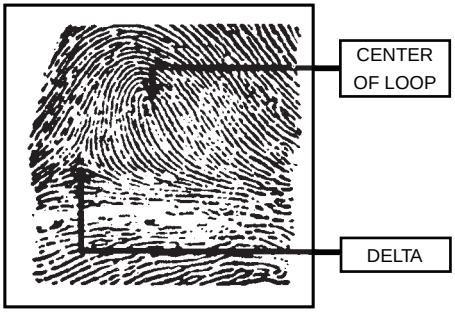
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY | L. THUMB | R. THUMB | RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY

1110-0046

FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE
CJIS DIVISION/CLARKSBURG, WV 26306

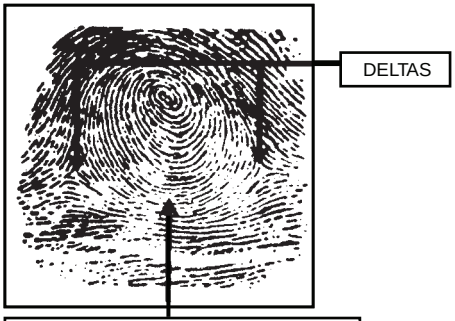
APPLICANT

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 I

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 J

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 K

Exhibit K

CONTACT INFORMATION

Print Management Branch

Lead:

Social Security Administration
Cheryl Tarver,
Room 3-B-9-D Annex Building,
6401 Security Boulevard, Baltimore, MD 21235-6401
Phone-(410)965-7253 Fax-(410)965-6400
Cheryl.tarver@ssa.gov

Technical Advisor:

Social Security Administration
Ken Wetzelberger
Room 3-B-9-G Annex Building,
6401 Security Boulevard, Baltimore, MD 21235-6401
Phone-(410)966-7109 Fax-(410)965-6400
Kenneth.wetzelberger@ssa.gov

Mail and Postage Policy Team

Social Security Administration
Attn: Renee Randall
3-E-9-H Annex Bldg.,
6401 Security Boulevard, Baltimore, MD 21235-6401
Phone-(410)965-1391 Fax-(410)965-6400
Renee.Randaall@ssa.gov

Social Security Administration
Attn: Tim Gimbel (Back-up)
6401 Security Boulevard, Baltimore, MD 21235-6401
Phone-(410)966-1738 Fax-(410)965-6400
Tim.Gimbel@ssa.gov

Help Desk

1-877-697-4978 or 1-877-697-4889

GPO

David Love
202-512-0307

dlove@gpo.gov

EXHIBIT L

Exhibit L

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

Exhibit L (cont'd)

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

EXHIBIT M

FedRAMP 3PAO Obligations and Performance Guide

FedRAMP

Version 1.0

July 29, 2015

FedRAMP 3PAO Obligations and Performance Guide

Revision History

Date	Version	Page(s)	Description	Author
07/29/2015	1.0	All	Initial Publication	FedRAMP

How to Contact Us

For questions about FedRAMP or this document, email to info@fedramp.gov.

For more information about FedRAMP, visit the website at http://www.fedramp.gov.

FedRAMP 3PAO Obligations and Performance Guide

1. INTRODUCTION

The Federal Risk and Authorization Management Program (FedRAMP) created a conformity assessment process to accredit Third-Party Assessment Organizations (3PAOs) to ensure that 3PAOs meet quality, independence, and knowledge requirements necessary to perform the independent security assessments required for FedRAMP. To maintain accreditation, 3PAOs must continue to demonstrate quality, independence, and FedRAMP knowledge as they perform security assessments on cloud systems.

2. 3PAO ACCREDITATION STANDARDS

3PAO accreditation by FedRAMP includes an assessment by the American Association for Laboratory Accreditation (A2LA). A2LA performs an initial assessment of each 3PAO required for accreditation by FedRAMP, a yearly surveillance, and a full re-assessment every 2 years for continued accreditation.

The A2LA assessment ensures that 3PAOs meet the FedRAMP requirements of ISO 17020 (as revised) and FedRAMP specific knowledge requirements related to the FedRAMP Security Assessment Framework. The A2LA provides an assessment report to FedRAMP that documents the 3PAO:

- Is competent to perform inspections of Cloud Service Provider (CSP) documents
- Has a documented and fully operational quality system
- Quality system meets the standards of ISO/IEC 17020-2012
- Is operating in accordance with its quality system

A2LA also assesses 3PAOs with specific FedRAMP and FISMA knowledge. A 3PAO must demonstrate technical competence through reviews of System Security Plans, creation of a Security Assessment Plan, and documenting the results in Security Assessment Test Cases as well as a Security Assessment Report.

3. 3PAO OBLIGATIONS

FedRAMP requires all 3PAOs to adhere strictly and continuously to the FedRAMP accreditation requirements and follow their ISO 17020 quality manual as described in their application and evaluated by A2LA. Among these requirements, a few key items are:

- The 3PAO must be independent from any CSP they assess. A 3PAO is only allowed to be a Type A or type C Inspection Body.
- All the assessment work that 3PAOs perform for CSPs must meet a high standard of independence and performance, especially quality, completeness, and timeliness.
- 3PAOs must demonstrate knowledge of FISMA and FedRAMP specific requirements when conducting their assessments.

3PAOs must continuously meet and demonstrate they are performing in accordance with these standards, which they demonstrated in their A2LA assessment. If a 3PAO has any questions on these matters, they should consult with FedRAMP.

FedRAMP 3PAO Obligations and Performance Guide

During a FedRAMP assessment, 3PAOs produce the following documents as a part of the overall security authorization package submitted for authorization to a government Authorizing Official:

- Security Assessment Plans (SAP)
  - Inventories
  - Rules of Engagement
- Security Assessment Reports (SAR)
  - Security Assessment Test Case Workbook
  - Risk Exposure Table
  - Penetration Test Report
  - Vulnerability Scan Data Files
  - Test Artifacts

These 3PAO documents must meet the following standards, reflective of their FedRAMP accreditation:

FedRAMP Standard	Details
Completeness	Complete and thoroughly prepared documents are expected on first submission. If any issues are identified, the 3PAO shall quickly and efficiently respond to the comments, and incorporate updates to resolve all the comments.
Timeliness	Documents are delivered on time, according to the schedule agreed to between the government, the CSP, and the 3PAO.
Standard templates	Documents are prepared using the most recent standard templates, without alterations or deletions, and insertions must be agreed upon.
Document Quality and Acceptance Criteria	The 3PAO must meet all quality and acceptance criteria as published by FedRAMP on the fedramp.gov website.
Testing Quality	Complete and accurate testing is an essential responsibility of a 3PAO. This responsibility derives from the 3PAO's A2LA assessment and the FedRAMP requirements for the highest quality testing.

Failure of a 3PAO to perform according to these standards affects the government's ability to authorize based on a 3PAO's assessment. FedRAMP will pursue corrective actions and possible removal of accreditations if 3PAO products do not meet the above standards.

4. 3PAO PERFORMANCE

The government evaluates all 3PAO products, and expects superior quality and performance. Quality is expected across the government, regardless of the whether a 3PAO is working directly with the FedRAMP PMO or JAB. In the event that a 3PAO's performance is not meeting

standards, FedRAMP has the authority and responsibility to pursue corrective actions, including the following:

FedRAMP Action	Details
Consultation	If a 3PAO has minor deficiencies in their performance: • FedRAMP will require a meeting with 3PAO representatives to discuss the specific deficiencies in the 3PAO's performance. • This will result in an internal Corrective Action Plan (CAP) being developed by the 3PAO and submitted to FedRAMP. • The CAP will be shared with A2LA during the 3PAOs next assessment.
Remediation	If a 3PAO has deficiencies in their performance or fails to complete the internal CAP: • A letter will be sent from the FedRAMP Director to the 3PAO notifying the 3PAO of specific deficiencies in 3PAOs performance. • This letter would also inform that the 3PAO's status is "In Remediation" and noted as such on www.FedRAMP.gov. • This letter will also require a 3PAO to provide a formal CAP to be submitted to FedRAMP within 7 days. • The CAP would need to include specific dates and actions for a 3PAO to complete in response the deficiencies noted in the letter from the FedRAMP Director. • As a part of this CAP, FedRAMP may require a re-assessment by A2LA for validation of the successful completion of the Corrective Action Plan.
Revocation	If a 3PAO has severe deficiencies in their performance or fails to complete a formal CAP from a "In Remediation" Status: • A letter will be sent from the FedRAMP Director to the 3PAO notifying the 3PAO of specific deficiencies in 3PAOs performance and that the 3PAO's status is being revoked and removed from the accredited list on www.FedRAMP.gov. • Revocations will last for a minimum of 6 months. • Revoked vendors are no longer authorized to provide assessment services to FedRAMP CSPs. • If 3PAO wishes to continue to be accredited, FedRAMP will require a 3PAO to commit to a formal CAP or revised CAP if revocation is due to failure to complete a CAP while in remediation status. • The CAP must include specific dates and actions for a 3PAO to correct the deficiencies noted in the letter from the FedRAMP Director and must be approved by the FedRAMP

FedRAMP Action	Details
	Director. • FedRAMP will require a re-assessment by A2LA for validation of the successful completion of the Corrective Action Plan.

5. REFERENCES

The following documents are references 3PAOs should review and incorporate in to their quality systems. These references will have regular updates as FedRAMP provides additional clarity and expectations.

- FedRAMP General Document Acceptance Criteria: The *FedRAMP General Document Acceptance Criteria* details general acceptance criteria for documents submitted to FedRAMP focused on clarity, completeness, conciseness, and consistency. Technical content is not addressed by these acceptance criteria.
- SAP Review Checklist: The *SAP Checklist* is a document that lists review items for SAP documents, specific to the SAP subject matter.
- SAR Review Checklist: The *SAR Checklist* is a document that lists review items for SAR documents, specific to the SAR subject matter.

FedRAMP 3PAO Obligations and Performance Guide

APPENDIX A: TABLE OF ACRONYMS

Acronym	Meaning
3PAO	Third-Party Assessment Organization
A2LA	American Association for Laboratory Accreditation
AO	Authorizing Official
ATO	Authority to Operate
CAP	Corrective Action Plan
CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
JAB	Joint Authorization Board
P-ATO	Provisional Authority to Operate
PMO	Program Management Office
SAP	Security Assessment Plan
SAR	Security Assessment Report

EXHIBIT N

PERFORATED PAYMENT STUB TO BE SUPPLIED AT POSTAWARD

EXHIBIT O

EXHIBIT O

Mail Run Data File (MRDF)

Or Item Level Accountability File

Record Descriptions		Position	Length
Job ID		1 – 5	5
Piece ID		6 – 11	6
Total Pages		12 – 13	2
Select Feeder 2	(0 = No Feed, 1 = Feed)	14	1
Select Feeder 3		15	1
Select Feeder 4		16	1
Select Feeder 5		17	1
Select Feeder 6		18	1
Select Feeder 7		19	1
Select Feeder 8		20	1
Select Feeder 9		21	1
Select Feeder 10		22	1
Vertical Stacker 1	(Seal envelope, do not meter)	23	1
Vertical Stacker 2	(Do not seal envelope, do not meter)	24	1
Vertical Stacker 3	(Overweight)	25	1
Vertical Stacker 4	(Trash)	26	1
Sealer	(0 = No Outsort, 1 = Outsort)	27	1
Meter 1	(0 = Print, 1 = No Print)	28	1
Meter 2		29	1
Customer Name		30	40
Address Line 1		70	40
Address Line 2		110	40
Address Line 3		150	40
Address Line 4		190	40
Address Line 5		230	40
Address Line 6		270	40
Zip Code		310	5
+4		315	4
+2		319	2
Return Name		321	40
Address Line 1		361	40
Address Line 2		401	40
Address Line 3		441	40
Address Line 4		481	40
Account ID		521	16
Input File Name		537	44
IMBC Codes		581	65
Service Type		646	3
IMBC SerialID		649	9
Filler		658	3
User Defined		661	29
Vendor ID		690	4
Code Name		694	5
Total Documents		699	2
End		701	1

NOTE: There is one record for each mail packet.

EXHIBIT P

SSA POSTAGE METER ACTIVITY LOG

CONTRACT NUMBER:

METER MANUFACTURER:

METER SERIAL NUMBER:

TODAY'S DATE	METER DATE	WORKLOAD MAILER NUMBER / NAME	SSA PRINT ORDER # / CONTRACTOR ORDER #	FILE DATE	BEGINNING METER BALANCE AMOUNT	METER REPLENISH-MENT AMOUNT (if applicable)	METER RATE	CERT. BULK MAILING CHARGES (if applicable)	TOTAL NUMBER OF PIECES METERED	SPOILED POSTAGE / POSTAGE ERRORS (actual cost)	TOTAL METER POSTAGE USED	ENDING METER BALANCE AMOUNT	NOTES