Program No 0856-S R-1 Term DATE OF AWARD To 03/31/18

TITLE: 0856-S

			AWRC dbe Post Masters		DATA INTERGRATORS		Gray Graphics		NPC, Inc.		PINNACLE DATA SYSTEMS, LLC	
			Indianapolis, IN		Fredericksburg, VA		Capitol Heights, MD		Claysburg, PA		Atlanta, GA	
			UNIT RATE	COST	UNIT RATE	COST	UNIT RATE	COST	UNIT RATE	COST	UNIT RATE	COST
		Basis of										
Item No.	Description	Award										
I.	**COMPOSITION:**											
(a)	Notices and Scannable Forms……………………………….per page	85	$ 10.00	$ 850.00	$ 20.00	$ 1,700.00	$ 15.00	$ 1,275.00	$ 15.00	$ 1,275.00	NC	-
(b)	Envelopes…………………………………………………….per envelope	15	$ 10.00	$ 150.00	$ 10.00	$ 150.00	$ 10.00	$ 150.00	$ 10.00	$ 150.00	NC	-
II.	**PRINTING/IMAGING AND BINDING, AND CONSTRUCTION:**											
(a)	*Makeready/setup charge……………………………………………………………………….per order	11	$ 150.00	$ 1,650.00	NC	$ -	$ 250.00	$ 2,750.00	$ 350.00	$ 3,850.00	NC	-
(b)	Notices and Scannable forms: Printing in black…………………………………..per 100 pages	81,321	$ 0.81	$ 65,870.01	$ 0.70	$ 56,924.70	$ 1.20	$ 97,585.20	$ 0.56	$ 45,539.76	$ 0.90	$ 73,188.90
(c)	Mail-out Envelopes: Printing in black, including construction……….per 100 envelopes	21,775	$ 0.80	$ 17,420.00	$ 0.70	$ 15,242.50	$ 1.00	$ 21,775.00	$ 0.80	$ 17,420.00	NC	-
(d)	CRM/BRM Envelopes: Printing in black, including construction ……per 100 envelopes	16,496	$ 0.80	$ 13,196.80	$ 0.60	$ 9,897.60	$ 0.80	$ 13,196.80	$ 0.62	$ 10,227.52	NC	-
III.	**PAPER:**											
(a)	Notices and Scannable form, White Offset (50 lb.)…………………………………………….per 100 leaves	52,793	$ 0.69	$ 36,427.17	$ 0.60	$ 31,675.80	$ 0.65	$ 34,315.45	$ 0.58	$ 30,619.94	$ 0.60	$ 31,675.80
(b)	Mail-out Envelope w/window, White (24 lb.) or White Offset Book, (60 lb.) ………..per 100 leaves	21,775	$ 1.76	$ 38,324.00	$ 0.60	$ 13,065.00	$ 2.00	$ 43,550.00	$ 1.50	$ 32,662.50	$ 2.10	$ 45,727.50
(c)	BRM/CRM Return Envelope, White Writing (20 lb.) or White Offset Book (50 lb)…..per 100 leaves	16,496	$ 1.35	$ 22,269.60	$ 1.20	$ 19,795.20	$ 1.25	$ 20,620.00	$ 0.62	$ 10,227.52	$ 1.20	$ 19,795.20
IV.	**INSERTING AND MAILING:**											
(a)	Mailers 1 through 11: Inserting of required materials for each mailer…………………….per 100 mailers	21,775	$ 3.00	$ 65,325.00	$ 2.40	$ 52,260.00	$ 2.00	$ 43,550.00	$ 3.00	$ 65,325.00	$ 2.00	$ 43,550.00
V.	**PRE-PRODUCTION TESTS:**											
(a)	Wire Transmission Test (per test)…………………………………………………………………………………………	1	$ 100.00	$ 100.00	$ 200.00	$ 200.00	$ 250.00	$ 250.00	NC	-	NC	-
(b)	Pre-production Validation Test (per test)…………………………………………………………………………………	1	$ 1,500.00	$ 1,500.00	$ 200.00	$ 200.00	$ 1,000.00	$ 1,000.00	NC	-	NC	-
	CONTRACTOR TOTALS			**$263,082.58**		**$201,110.80**		**$280,017.45**		**$217,297.24**		**$213,937.40**
	DISCOUNT		0.00%	**$0.00**	2.00%	**$4,022.22**	2.00%	**$5,600.35**	0.25%	**$543.24**	1.00%	**$2,139.37**
	DISCOUNTED TOTALS			**$263,082.58**		**$197,088.58**		**$274,417.10**		**$216,754.00**		**$211,798.03**

Program No 0856-S R-1 Term DATE OF AWARD To 03/31/18

TITLE: 0856-S

			SourceLink Ohio, LLC		NPC	
			Miamisburg, OH		Claysburg, PA	
			UNIT RATE	COST	UNIT RATE	COST
		Basis of			Current Contractor	
Item No.	Description	Award				
I.	**COMPOSITION:**					
(a)	Notices and Scannable Forms……………………………….per page	85	$ 10.00	$ 850.00	$ 20.00	$ 1,700.00
(b)	Envelopes…………………………………………………….per envelope	15	$ 10.00	$ 150.00	$ 10.00	$ 150.00
II.	PRINTING/IMAGING AND BINDING, AND CONSTRUCTION:					
(a)	*Makeready/setup charge……………………………………………………………………….per order	11	$ 500.00	$ 5,500.00	$ 500.00	$ 5,500.00
(b)	Notices and Scannable forms: Printing in black…………………………………..per 100 pages	81,321	$ 0.92	$ 74,815.32	$ 0.72	$ 58,551.12
(c)	Mail-out Envelopes: Printing in black, including construction……….per 100 envelopes	21,775	$ 0.69	$ 15,024.75	$ 0.82	$ 17,855.50
(d)	CRM/BRM Envelopes: Printing in black, including construction ……per 100 envelopes	16,496	$ 0.73	$ 12,042.08	NEW	$ -
III.	**PAPER:**					
(a)	Notices and Scannable form, White Offset (50 lb.)…………………………………………….per 100 leaves	52,793	$ 0.70	$ 36,955.10	$ 0.61	$ 32,203.73
(b)	Mail-out Envelope w/window, White (24 lb.) or White Offset Book, (60 lb.) ………..per 100 leaves	21,775	$ 1.21	$ 26,347.75	$ 1.34	$ 29,178.50
(c)	BRM/CRM Return Envelope, White Writing (20 lb.) or White Offset Book (50 lb)…..per 100 leaves	16,496	$ 1.04	$ 17,155.84	$ 0.97	$ 16,001.12
IV.	**INSERTING AND MAILING:**					
(a)	Mailers 1 through 11: Inserting of required materials for each mailer…………………….per 100 mailers	21,775	$ 2.23	$ 48,558.25	$ 3.15	$ 68,591.25
V.	**PRE-PRODUCTION TESTS:**					
(a)	Wire Transmission Test (per test)…………………………………………………………………………………………	1	$ 1.00	$ 1.00	NC	$ -
(b)	Pre-production Validation Test (per test)…………………………………………………………………………………	1	$ 200.00	$ 200.00	$ 1,000.00	$ 1,000.00
	CONTRACTOR TOTALS			**$237,600.09**		**$230,731.22**
	DISCOUNT		0.00%	**$0.00**	0.25%	**$576.83**
	DISCOUNTED TOTALS			**$237,600.09**		**$230,154.39**

U.S. GOVERNMENT PUBLISHING OFFICE
Washington, DC

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

Mid-Year Mailer (MYM) OCR Forms Notices
National Change of Address (NCOA) Notices
Step Parent Notices
Fee Adjustment Notices

As requisitioned for 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 Date of Award and ending March 31, 2018, plus up to four (4) optional 12-month extension periods that may be added in accordance with the "OPTION TO EXTEND THE TERM OF THE CONTRACT" clause in SECTION 1 of this contract.

NOTE: Contract interfacing with SSA's National File Transfer Management System (FTMS) for electronic transmission of files from SSA to the production facility will commence from Date of Award and must be completed no later than 90 workdays prior to start of live production. Transmission of live production files will commence on June 30, 2017.

BID OPENING: Bid shall be publicly opened at 11:00 a.m., prevailing Washington, DC time, on March 10, 2017.

BID SUBMISSION: Submit bid in pre-addressed envelope furnished with solicitation, or send to: U.S. Government Publishing Office (GPO), Bid Section, Room C-848, Stop: CSPS, 732 North Capitol Street. NW Washington, DC 20401-0001. Facsimile bids in response to this solicitation are also permitted. Facsimile bids may be submitted directly to the GPO Bid Section, Fax No. (202) 512-1782. The program number (856-S) and bid opening date must be specified with the bid. Refer to Facsimile Bids in Solicitation Provisions of GPO Contract Terms, GPO Publication 310.2, as revised June 2001. Hand delivered bids are to be taken to: GPO Bookstore, 710 North Capitol St. NW Washington, DC 20401 between the hours of 8:00 a.m. and 4:00 p.m., Monday through Friday. The contractor is to follow the instructions in the Bid Submission/Opening Area. If further instruction or assistance is required call (202) 512-0526.

NOTE: The products produced in this contract were formerly procured under Program 391-S. The specifications have been extensively revised; therefore, all bidders are cautioned to familiarize themselves with all provisions of these specifications and are strongly encouraged to ask questions regarding the program requirements prior to bidding.

Abstracts of contract prices are available at http://www.gpo.gov/gpo/abstracts/abstract.action?region=DC.

For information of a technical nature, call Kevin Hodges at (202) 512-0310; or email khodges@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 Publications 310.2, effective December 1, 1987, Rev. 6-01) and GPO Contract Terms, Quality Assurance through Attributes Program for Printing and Binding (GPO Publications 310.1, effective May 1979, Rev. August 2002).

GPO Contract Terms (GPO Publications 310.2) http://www.gpo.gov/pdfs/vendors/sfas/terms.pdf

GPO QATAP (GPO Publications 310.1) http://www.gpo.gov/pdfs/vendors/sfas/qatap.pdf

DISPUTES: GPO Publication 310.2, GPO Contract Terms, Contract Clause 5. Disputes, is hereby replaced with the June 2008 clause found at www.gpo.gov/pdfs/vendors/contractdisputes.pdf.

SUBCONTRACTING: The predominant production functions are the laser/ion deposition of variable data at a minimum of 600 x 600dpi for notices, the printing/imaging of notices, and the inserting of items into mail-out envelopes. Any bidder who cannot perform the predominant production functions will be declared non-responsible.

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

NOTE: If the presorting and mailing is subcontracted, the subcontractor must have the same security clearance as the primary contractor.

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

If the contractor plans to enter into a "Contractor Team Arrangement", or Joint Venture, to fulfill any requirements of this contract, all parties must comply with the terms and regulations as detailed in the Printing Procurement Regulation (GPO Publication 305.3; Rev. 2-11).

QUALITY ASSURANCE LEVELS AND STANDARDS: The following levels and standards shall 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 Z1.4):

(a) Non-destructive Tests - General Inspection Level I.

(b) Destructive Tests - Special Inspection Level S-2.

(c) Transparent: low-gloss poly-type window material, covering the envelope window must pass 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)" shall apply to these specifications. The revisions of this standard that are effective as of the date of this contract are those, which shall apply.

(e) Exception: The PDF417 2-D barcodes must be in accordance with the requirements of ANSI MH 10.8.3M unless otherwise specified.

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

NOTE: The scannable forms produced under these specifications must be guaranteed to function properly when processed through the WBDOC Integrated Based Data Capture System (IIDBCS). The bar coding must be readable by all standard barcode scanning devices regardless of the contractor's method of reproducing the codes. SSA's current equipment: WDR Reader – Worthington Data Solutions and High Speed Scanners. **Forms require precision spacing, printing, trimming and folding to guarantee proper processing.**

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

	Attribute	Specified Standard
P-7.	Type Quality and Uniformity	O.K. Press Sheet
P-8.	Solid and Screen Tint Color Match	O.K. Press Sheet

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

P-7.	O.K. Proofs, Electronic Media, Camera Copy, Manuscript Copy.
P-8.	Pantone Matching System

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 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 as may be mutually agreeable to 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 Date of Award to March 31, 2018, 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 December 31, 2016, called the base index. The percentage increase or decrease against the total price of 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 reimbursement 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 6 – 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:

1. BLS code 0913-01 for Offset and Text will apply to all paper required under this contract.
2. The applicable index figures for the month of March 2017 will establish the base index.
3. There shall be no price adjustment for the first three production months of the contract.
4. Price adjustments may be monthly thereafter, but only if the index varies by an amount (plus or minus) exceeding 5% by comparing the base index to the index for that month which, is two months prior to the month being considered for adjustment.
5. Beginning with order placement in the fourth month, index variances will be calculated in accordance with the following formula:

$$\frac{X - \text{base index}}{\text{base index}} \times 100 = \_\_\_\_\%$$

where X = the index for the 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 line items III. (a), (b), and (c) 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 allowances for any contingency to cover anticipated increased costs of paper to the extent such increases are covered by this price adjustment clause.

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 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 retrieved any such records.

(c) The contractor must 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. Section 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 employees may also be subject to the criminal penalties As set forth in that provision.

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

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

A copy of this signed certification must be forwarded to: SSA. T. Marshall-Vanzego, DPAMS, 1343 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401.

A copy must also be forwarded to: U.S. GPO, 732 North Capitol Street, NW, CSAPS, DCT 1, Room C-838, Washington, DC 20401. Attn: Kevin Hodges

(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 on this contract, the subcontractor must conform to all security requirements as that of the contractor.

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.

"United States" means the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, 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 Division of Printing Management (See Exhibits), the contractor 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 Management Act (FISMA) to develop security standards for federal information processing systems, and Office of Management and Budget (OMB) Circular A-130 Appendix III.

(d) Solutions 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, CSP's must have a security control assessment performed by a Third Party Assessment Organization.

NOTE: A Third Party Assessment Organization (3PAO) is an organization that has been certified to help cloud service providers and Government agencies meet FedRAMP compliance regulations. Accredited 3PAOs can be found at https://www.fedramp.gov/marketplace/accredited-3paos/.

(e) Before SSA provides data to the contractor, the contractor shall submit a System Security Plan (SSP) which 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 which requires the use of NIST SP 800-53, or the contractor shall provide a Security Assessment Package (SAP) completed by either an independent assessor or another Federal agency.

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.

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

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: See Exhibits for References for External Service Providers (ESP).

PHYSICAL SECURITY: Contractor's facilities storing SSA assets and information are required to meet the Interagency Security Committees (FSC) 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 60 calendar days of notification. Requirements can include but are not limited to, the following physical security countermeasures: access control systems, closed circuit television systems, intrusion detection systems, and barriers.

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.

All employees working on this contract must:

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

Contractor's managers working on this contract must:

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

Applicability:

The responsibility to protect 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 written 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 personally identifiable information is not properly safeguarded:

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

This list does not encompass all failures to safeguard 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 personally identifiable information, they should consult the Contracting Officer or the Contract Administrator.

PUBLIC TRUST SECURITY REQUIREMENTS: This contract has been designated Public Trust Position Level 5C. Due to the sensitive nature of the information contained in the products produced under this contract. Contractor employees performing under this contract will be subject to a thorough civil and criminal background check.

"Performing under this contract" is defined as either working on-site at an SSA facility (including visiting the SSA site for any reason) or having access to Government programmatic or sensitive information.

Within two (2) days following contract award, the contractor must provide to SSA an Electronic Questionnaire for Investigation (eQIP) applicant listing of all individuals for whom the contractor is requesting a suitability determination (i.e., background investigation). This listing should include the following:

- Contractors' name
- Contract number
- Contractor's point of contact (CPOC) name
- CPOC's contact information including email address
- Each applicant's full name, Social Security Number (SSN), date of birth, and 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.)

The background investigation process will not start until the applicant listing is submitted. Send the applicant listing via fax to Center for Personnel Security and Project Management (CPSPM) Suitability Team (410) 966-0640 or via U.S. Mail to: Social Security Administration, CPSPM Suitability Team, 2601 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235.

Once SSA receives and reviews the applicant listing, SSA will initiate the eQIP. SSA will Email notification to the CPOC the name of each applicant invited into the eQIP website to complete their background investigation form. The CPOC will provide the website to the applicants to complete their eQIP form electronically. **The applicant will have up to 14 calendar days following SSA notification to the CPOC of the eQIP invitations to complete the eQIP form.**

The applicant must print the signature pages of the SF 85P form (pages 7 through 9) prior to releasing the application in eQIP, sign the signature pages and provide the signed originals to the CPOC. (see Exhibits)

The following is a list of documents the contractor employees will be responsible for completing:

- Original signed and dated eQIP signature pages as specified in the above paragraph.
- Two (2) "Fingerprint Cards" (FD-258, see Exhibits), NOTE: The contractor will absorb the costs for obtaining fingerprints.
- One (1) "Declaration for Federal Employment" (Optional Form 306, see Exhibits).
- One (1) "Fair Credit Reporting Act Authorization Form" (FCRA, see Exhibits).
- For a non-U.S. citizen, one (1) legible photocopy of the work authorization permit and social security card

The CPOC must ensure all paper forms are fully completed and signed prior to submission to SSA. All forms and fingerprinting cards must be submitted at least 15 workdays prior to the date work is to begin on the contract. Fingerprint cards and all paper forms must be legible or typed in black ink and all signatures must be in black ink. There must be no "breaks" in residences or employment. SSA requires complete addresses, including zip codes, and phone numbers with area code. SSA must receive forms and fingerprint cards within 30 calendar days after notification of the eQIP invitation. It is the responsibility of the contractor to ensure fingerprint cards are processed through their local police departments or other authorized finger printers. SSA will return incomplete forms back to the contractor. Forms may be obtained by calling SSA Personnel Security Suitability Program Officer (SPO) Vernon Collins at (410) 965-3329.

The CPOC will submit one cover sheet containing the names of all of the individuals for whom the contractor is submitting completed paperwork. This cover sheet should include the contract number, each applicant's full name, each applicant's Social Security Number (SSN), each applicant's date of birth, and each applicant's place of birth. The CPOC will submit this cover sheet along with the completed paper forms and two FD-258 fingerprint charts for each applicant via U.S. Mail to: SSA, CPSPM Suitability Team, 2601 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235.

Simultaneously, The CPOC will also email a copy of the cover sheet ONLY to the Contracting Officer Technical Representative (COTR) at SSA DPAMS (see, Exhibits). Before forwarding, the CPOC will remove all personal information from the applicant list (SSN, date of birth, and place of birth).

NOTE: IT IS THE RESPONSIBILITY OF THE CPOC TO ENSURE CLEARANCES ARE OBTAINED PRIOR TO ANY CONTRACT TESTING.

The CPOC will follow this instruction for new contract employees hired during the contract term.

Suitability Determination:

A Federal Bureau of Investigation fingerprint check is part of the basis used 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 contractor personnel unsuitable to continue performing under this contract. CPSPM will notify the CPOC, COTR, and CO of the results of these determinations.

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 of all of the contractor's computer, printing, and mailing equipment utilized on this contract or to require other evidence of technical, production, managerial, financial, and similar abilities to perform, prior to the award of a contract.

The preaward survey will include a review of all subcontractors involved, along with their specific functions; and the contractors/subcontractor's mail, material, personnel, production, quality control/recovery program, security, and backup facility plans, as required by this specification.

If award is predicated on the purchase of production and/or systems equipment, the contractor must provide purchase order(s) with delivery date(s) of equipment to arrive, be installed, and fully functional at least 45 calendar days prior to the start of live production.

PRODUCTION PLANS: The contractor shall present, in writing, to the Contracting Officer within 10 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.

THESE PROPOSED PLANS ARE SUBJECT TO REVIEW AND APPROVAL BY THE GOVERNMENT AND AWARD WILL NOT BE MADE PRIOR TO APPROVAL OF THE SAME.

NOTE: THE GOVERNMENT RESERVES THE RIGHT TO WAIVE SOME OR ALL OF THESE PLANS.

Backup Facility: The failure to deliver these notices/forms 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, 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 notices/forms.

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.

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 cover the security over the postage meters as well as the controls for the setting of the meters.

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 back-up 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 (minimum pull- first from each file and then one every 4,000 notices) the contractor intends to utilize. The contractor will perform programming to create two duplicate notices at set intervals throughout production and diverted samples at the insertion stage to complete the following:

- One (1) sample will be inspected and tested by both the press crew and an independent Quality Assurance Technician who will evaluate compliance of diverted product to contract specifications for the duration of the job.
- One (1) sample will be drawn for the Social Security Administration and will be packed with associated pieces from each print order and shipped weekly, within three (3) workdays of completion of each print order, to the Social Security Administration. (Address to be supplied at the post award meeting).

The plan shall detail the actions to be taken by the contractor when either 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. 6-01)).

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 120 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 for electronic transmission of files from SSA. The plan must also include the media type on which files from SSA will be received to the extent that operator intervention (e.g., a tape mount) is not required at SSA or the contractor's production facility.

The system plan shall demonstrate the contractor's ability to provide complete hardware and software compatibility with SSA's existing network (see "WIRE TRANSMISSIONS" for additional information). The contractor must complete a System Plan (see Exhibits).

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.

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 automated 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 pick-up/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:

(a) list of all production equipment and equipment capacities to be utilized on this contract;

(b) the production capacity currently being utilized on this equipment;

(c) capacity that is available for these workloads; and,

(d) if new equipment is to be utilized, documentation of the purchase order, source, delivery schedule, and installation dates are required – 90 calendar days prior to start of contract.

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 subcontractors proposed plans, which are subject to review and approval by the Government.

NOTE: 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 15 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.

Contractors are 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. Contractors classified as Cloud Service Providers (CSP) must adhere to additional FedRAMP security control requirements. CSPs must have a security control assessment performed by a Third Party Assessment Organization (3PAO) (see Exhibits), additional information is also available at http://www.gsa.gov/portal/category/102371.

5. The contractor shall submit a System Security Plan which 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 which requires the use of NIST SP 800-53 or the contractor shall provide a Security Assessment Package completed by either an independent assessor or another Federal agency.

Material/Production Area: The contractor must provide a secure area(s) dedicated to the processing and storage of data for notices, either a separate facility dedicated to this product, 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 notices.

Part of the Security Control 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 plans.

Disposal of Waste Materials: The contractor is required to demonstrate how all waste materials used in the production of sensitive SSA records 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. Definitively *destroying* the records means the material cannot be reassembled and used in an inappropriate manner in violation of law and regulations. Sensitive records are records that are national security classified or exempted from disclosure by statue, including the Privacy Act or regulation.

The contractor, at a minimum, must crosscut shred all documents into squares not to exceed one-quarter inch. All documents to be destroyed cannot leave the security of the building and must be destroyed 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. This sample must have a unique number and must be produced on each notice. The contractor will generate a list of the unique identifying numbers for each sample. As samples are pulled, the unique numbers will be marked off the list. This enables the contractor to track which samples have been produced and pulled and what records have been produced. Mail test samples directly to SSA, DPAMS, Attn: T. Marshall-Vanzego, 1343 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235- 6401.

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

RECOVERY SYSTEM: A recovery system will be required to ensure that all defective, missing, or mutilated pieces detected are identified, reprinted, and replaced. The contractors' 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 USPS facility. An explanation of the contractor's sequential numbering system is required to understand the audit trail required for every piece.

100% ACCOUNTABILITYOF 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.

NOTE: Contractor must have all hardware, programming and finalized reports in place to meet this requirement and arrive at least 90 calendar days prior to the start of live production, on or near June 1, 2017. Contractor must submit a sample of their proposed Audit and Summary reports with the required preaward production plans for approval. The Government considers grounds for the immediate default of this contract if the contractor, at any time, is unable to perform or found not complying with any part of this requirement.

Notice integrity shall be defined as follows:

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

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

Mailing integrity shall be defined as follows:

- All notices received from SSA for each file dates that 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, and that 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 the following:

(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: Due to inserting equipment limitations, the contractor can divert and insert by hand notices over 50 leaves. These notices, to ensure notice integrity, are to be scanned and collated by an automated process prior to manual handling for inserting. The completed mail package must then be processed through exit scanning. The event log report must show these as 50+ Manual.

(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 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 and verification 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, and 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 six-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 leave, 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, 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.

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

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

NOTE: A PDF copy of the summary report(s) and matching USPS 3607R and/or GPO 712 form(s) must be submitted to SSA, DPAMS, Baltimore, MD, (see Exhibits) for each file date within 24 hours of mailing.

NOTE: Contractor must submit a sample of their Audit and Summary reports (see Exhibits) 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 MS Word, MS Excel, or PDF.

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 180 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 FOREIGN NOTICES PULLS FROM FILE PRIOR TO PRODUCTION: The contractor is to remove foreign notices from files transmitted prior to production of the files.

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

The contractor will be required to provide one private office of not less than 150 square feet, furnished with at least one (1) desk, two (2) swivel arm chairs, secure internet access for Government laptop computers, a work table, and two (2) four-drawer letter-size files with combination padlock, Pendaflex file folders, or equal.

On-site representative(s) may be stationed at the contractor's facility to: provide project coordination in receipt of wire 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 coordinators will not have contractual authority, and cannot make changes in the specifications or in contract terms, but will bring all defects detected to the attention of the company Quality Control Officer. The coordinators must have full and unrestricted access to all production areas where work on this program is being performed.

POSTAWARD CONFERENCE: In order to ensure that the contractor fully understands the total requirements of the job as indicated in these specifications, Government representatives will conduct a conference with the contractor's representatives at the Social Security Administration, Baltimore, MD, immediately after award.

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

PREPRODUCTION MEETING: A preproduction meeting covering the printing, imaging, folding, inserting, and mailing shall 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 shall present and explain their final plan for the printing, imaging, folding, inserting, and mailing.

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

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

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

ASSIGNMENT OF JACKETS, PURCHASE, TASK ORDERS 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 electronic "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 Date of Award through March 31, 2018, 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 (GPO Form 2511) will be used for billing purposes, will be issued weekly, and will cover all daily task orders issued that week.

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.

Upon completion of mailing contractor must invoice within 72 hours. Processing invoices for payment, fax the completed invoice to GPO by utilizing the GPO barcode coversheet program application. Access the hyperlink below and follow the instructions as indicated:

http://winapps.access.gpo.gov/fms/vouchers/barcode/instructions.html

Facsimile transmission should only be used when no samples are required with contractors invoice, otherwise payment will be held up while the invoice is returned to the contractor for the required sample(s).

All invoice packages and envelopes MUST be mailed to: U.S. Government Publishing Office COMPTROLLER-FMCE, Office of Financial Management, Washington, DC 20401.

Contractor must provide pdf copies of the billing payment invoice form 1034 showing amount of billing invoice to SSA, DPAMS (see Exhibits).

Note: Do not mail billing invoices to any other GPO Procurement Office as this will delay payment.

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.

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.

SECTION 2 – SPECIFICATIONS

SCOPE: These specifications cover the production of mailing packages from four (4) identified workloads consisting of a personalized English or Spanish notice and any combination of a personalized OCR scannable form, a Courtesy Reply Mail (CRM) return envelope, a Business Reply Mail (BRM) return envelope, and a mail-out envelope, which require such operations as the receipt and processing of files; composition; printing; variable imaging in black ink (computerized printing with 2D barcodes); folding; inserting; and, mailing.

The forms produced under these specifications require precision spacing, printing, and trimming and must be guaranteed to function properly when processed through the WBDOC Integrated Image Based Data Capture System (IIBDCS). The barcoding must be easily readable by all standard bar code scanning devices regardless of the contractor's method of reproducing the codes. (SSA equipment: WDR Reader – Worthington Data Solutions and High Speed Scanners.)

The following equipment will be used for extracting the OCR forms from the CRM envelopes: OPEX MPE 7.5 Multiple Purpose Extractor.

The four (4) identified workloads thus far are as follows:

1. Mid-Year Mailer OCR Form Notices
2. National Change of Address Notices
3. Step Parent Notices
4. Fee Adjustment Notices

Future Workload(s):

5. New Notices (during the term of the contract)

NOTE: 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.

- These new mailers could be English and/or Spanish notices.
- Notices will consist of 1 to 8 pages (no more than 4 leaves).
- These mailers may consist of a personalized notice and mail-out envelope or a personalized notice, mail-out envelope
- CRM return envelope and BRM envelope.
- All notice and envelope requirements will match those described in Mailers 1 through 4.

<u>DATA SET NAME</u> *

The file name may be in the following formats ("vendor" would be an SSA-assigned vendor identifier):

OLBG.BTO.filename.vendor.RYYMMDD

*The actual data set names will be provided to the contractor at the postaward meeting.

All files will be electronically transmitted to the contractor. 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 each of SSA's validations.

NOTE: The contractor must not compress files in processing data for this contract. The contractor must print the address record exactly as it is in the Master Beneficiary Record (MBR) file furnished to the contractor. The contractor must not standardize the addresses or change the ZIP+4 information.

FOR QUALITY CONTROL AND AUDITING PURPOSES:

All files transmitted by SSA will be physical sequential. Any alteration of the notice content in the file is not permitted.

FREQUENCY OF ORDERS:

Mid-Year Mailer Notices: There will be 5 orders per year. Each year, the orders will transmit in June, July, August, October, and November) with the majority of the quantity transmitting in July.

NCOA Notices: There will be 4 orders per year. Each year, the orders will transmit in March, June, September and December.

Step Parent Notices: There will be 1 order per year. Each year, the order will transmit in the month of December. All notices must mail on or before December 31st of each year.

Fee Adjustment Notices: There will be 1order per year. Each year, the order will transmit in the month of November. All notices must mail on or before December 1st of each year.

Any certified mail files for the following workloads above will mail only when required and can occur with any of the print orders.

QUANTITY/NUMBER OF LEAVES AND PAGES:

Combined total for the Mid-Year Mailer (MYM) OCR Notices, NCOA Notices, Step Parent Notices and Fee Adjustment Notices will be approximately 2,177,450 notices per year. All quantities and page numbers listed below are approximate. Actual quantities and page numbers are not known until files are delivered.

1. Mid-Year Mailer OCR Notices workload has 4 mailers consisting of 12 different mail packages, each consisting of a combination of components listed below:

- Personalized English or Spanish notice
- Personalized OCR scannable form
- Courtesy Reply Mail return envelope
- Business Reply Mail return envelope
- Mail-out envelope

Mailer/Notice	Transmits	Quantity	Leaves	Printed Pages
M1 - SSA-131-SM-SUP Scannable Form	June	55,000	2	3
M2 – SSA-L9790	June	72,000	3	4
M3 – SSA-L9778-SM-SUP	July	47,000	4	7
SSA-L9779-SM-SUP	July	152,000	4	8
SSA-L9781-SM-SUP	July	1,260	3	5
SSA-L9784-SM-SUP	July	14,000	3	6
SSA-L9785-SM-SUP	July	375,000	4	8
M3 –SSA-L9781-SM-SUP	Aug	30,000	4	8
	Sep	30,000	4	8
	Oct	30,000	4	8
Total Yearly Quantities		806,260		

Note: Mailer 3 has a different CRM for each form. These same CRM's are also used for Mailer 4.

Mailer/Notice	Transmits	Quantity	Leaves	Printed Pages
M4 – SSA-L9778-SM-SUP-SP	July	1,700	4	7
SSA-L9779-SM-SUP-SP	July	6,700	4	8
SSA-L9781-SM-SUP-SP	July	20	3	5
SSA-L9784-SM-SUP-SP	July	120	3	6
SSA-L9785-SM-SUP-SP	July	8,500	4	8
M4 – SSA-L9781-SM-SUP-SP	Aug	500	4	8
	Sep	500	4	8
	Oct	500	4	8
Total Yearly Quantities		18,540		

2. National Change of Address Notices workload has two (2) mailers consisting of four (4) different mail packages. There are a total of 16 different variations possible. Each consisting of a combination of components listed below:

- Personalized English or Spanish notice
- Mail-out envelope

Mailer/Notice	Transmits	Quantity	Leaves	Printed Pages
M5 - SSA-L292-SM	Mar	275,360	1	1
SSA-L292-SM-SP	Mar	7,067	1	1
SSA-L292-SM	Jun	275,360	1	1
SSA-L292-SM-SP	Jun	7,067	1	1
SSA-L292-SM	Sep	275,360	1	1
SSA-L292-SM-SP	Sep	7,067	1	1
SSA-L292-SM	Dec	275,360	1	1
SSA-L292-SM-SP	Dec	7,067	1	1
Total Yearly Quantities		1,129,708		

Mailer/Notice	Transmits	Quantity	Leaves	Printed Pages
M6 - SSA-L294-SM	Mar	16,984	1	1
SSA-L294-SM-SP	Mar	774	1	1
SSA-L294-SM	Jun	16,984	1	1
SSA-L294-SM-SP	Jun	774	1	1
SSA-L294-SM	Sep	16,984	1	1
SSA-L294-SM-SP	Sep	774	1	1
SSA-L294-SM	Dec	16,984	1	1
SSA-L294-SM-SP	Dec	774	1	1
Total Yearly Quantities		71,032		

3. Step Parent Notices workload has three (3) different mail packages, each consisting of a combination of components listed below:

- Personalized English or Spanish notice
- Mail-out envelope

Mailer/Notice	Transmits	Quantity	Leaves	Printed Pages
M7 - SSA-L253-SM	Dec	650	1	1
M8 - SSA-L253-SM-SP	Dec	30	1	1
M9 - SSA-L253-SM-F	Dec	5	1	1
Total Yearly Quantities		685		

4. Fee Adjustment Notices workload has two (2) different mail packages, each consisting of a combination of components listed below:

- Personalized English or Spanish notice
- Mail-out envelope

Mailer/Notice	Transmits	Quantity	Leaves	Printed Pages
M10 - SSA-L251-SM *	Nov	150,000	1	1
M11 - SSA-L252-SM	Nov	1,225	1	1
Total Yearly Quantities		151,225		

* This notice will not occur in years when there is no Cost of Living Adjustment (COLA) announced. The number shown is an estimate if COLA is provided.

The quantities above per mailer are approximates and are based on historical data and are for the purpose of establishing a basis of award. Exact quantities by mailer are not known in advance and will be furnished with live production files. NO SHORTAGES WILL BE ALLOWED.

The Government reserves the right to increase by up to 20% the total number of notices ordered annually. This 20% includes the additional notices occasioned by the one (1) to three (3) new notice workloads developed during the term of this contract.

TRIM SIZES:

Notices:	8-1/2 x 11 (folding down to 8-1/2 x 5 1/2).
Scannable Forms:	8-1/2 x 11 (folding down to 8-1/2 x 5 1/2).
CRM Return Envelope:	5-3/4 x 8-3/4, plus flap. Six (6) different versions
BRM Return Envelope:	5-3/4 x 8-3/4, plus flap. One (1) version only
Mail-Out Envelopes:	6-1/4 x 9-1/2, plus flap. Eight (8) different versions

Certified and Registered Mail mailers: Mailers 1 through 11, when required, will have a duplicate, separate file transmitted at the same time as each of the above named mailers. The contractor must process these files separately as certified mail files or in the case of foreign mail as registered mail files, in accordance with the Special Mailing Requirements section of this contract. Certified and registered mail is anticipated to be less than 2% of total annual contract quantity.

GOVERNMENT TO FURNISH:

Manuscript copy for all 21 notices, one (1) scannable form, and 15 envelopes

Camera copy for the Facing Identification Mark (FIM), Intelligent Mail Barcode (IMB), and “Postage and Fees Paid” mailing indicia.

Camera copy for notice signatures

Camera copy for the recycled paper logo and legend (English and Spanish)

PS Form 3615, Mailing Permit Application and Customer Profile

Official Government Postage Meters

CASS Certification

NCOA Certificate

GPO Form 712 (Certificate of Conformance)

GPO Form 892 proof label

Exhibit A: Form SSA-301, Contractor Personnel Security Certification

Exhibit B: System Plans

Exhibit C: Sequence Summary/Audit Reports

Exhibit D: Questionnaire for Public Trust Positions (Standard Form 85P)

Exhibit E: Fingerprint Card (FD-258)

Exhibit F: Declaration of Federal Employment (Optional Form 306)

Exhibit G: Fair Credit Reporting Act Authorization Form

Exhibit H: Database/Spreadsheet for Postal Documentation

Exhibit I: SSA and GPO Personnel Contact Information

Exhibit J: Production spreadsheet

Exhibit K: Vendor Record Specifications for each workload

Exhibit L: Reference for External Service Providers (ESP)

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.

Identification markings such as register marks, ring folios, rubber-stamped jacket numbers, commercial identification marks of any kind, etc., except GPO imprint, form number, and revision date, carried on copy, or in electronic files must not print on finished product.

COMPOSITION: The contractor will be required to set type for all components (notices, OCR scannable forms, and envelopes) of each of the mailers. Contractor will be required to set type for 15 envelopes. Helvetica or similar typeface will be utilized.

Contractor to set type for 11 notices and OCR form (approximately 85 pages) within each, flushed left, and ragged right. The laser imaging must not be conspicuously different in quality from images produced by photocomposition and must have a minimum resolution of 300 x 300 dpi. Set type in Century Schoolbook, Times Roman, or similar Serif typeface. Use the largest type size possible for the space available. No alternate typefaces will be allowed; however, manufacturers' generic equivalents will be accepted for the above typefaces.

For the OCR scannable forms, exact spacing and locations of scan boxes and variable data must be maintained for readability of pre-programmed scanning equipment. The spacing and page layout of the form must be consistent between each English and Spanish form version although the contractor may vary font size between the English and Spanish form to fit available space.

NOTE: Image position of all variable and/or static type matter, and data on the OCR scannable forms must meet GPO Quality Assurance Level III requirements. Form work will be defined as matter set in all sizes, and will include vertical, horizontal, and diagonal rules, box-heads, numbered lines, checkboxes, arrows, type matter, manuscripts, etc., positioned in the proper location to provide spaces for information to be filled in individually.

Font for Intelligent Mail Barcode (IMB) is required.

PROOFS: Samples (25 of each) of all notices and/or form for any mailers will be required on the first print order of each mailing. Samples may be imaged on white paper and contain variable information or in PDF format. It will be at the discretion of SSA if one or both proofing methods will be used.

Six (6) sets of digital content proofs of all components (scannable OCR form, personalized notices, and envelopes) will be required. Proofs must be created using the Raster Image Processor (RIP) that will be used to produce all products. Proofs must be collated with all elements in their proper position (not pasted up), imaged face and back, trimmed and folded to the finished size of the product. Proofs must also indicate margins.

Notices and Scannable forms: Three (3) printed samples, in black ink, of all notices and forms.

When ordered, one (1) set of Adobe Acrobat version 9.0 (or later version) soft proofs. Proofs will be transferred to the agency via email. The PDF proof will be evaluated for text flow, image position and color breaks. Proofs will not be used for color match.

PDF proofs of all items for all mailers will be required in the form of one (1) set of Adobe Acrobat version 9.0 (or later version) soft proofs. Government has the option to request hard copy proofs as needed in which the contractor must deliver within 48-hours upon receipt of request.

SSA reserves the right to make changes to all proofs. The Government may require one (1) or more sets of revised proofs before rendering an “OK TO PRINT”.

NOTE: Proofs will be required with the initial order and any time that a copy change is required during the term of the contract.

If any contractor’s errors are serious enough in the opinion of the GPO to require revised envelope proofs, the revised envelope 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.

Note: The contractor must not print prior to receipt of an “O.K. to print.”

WIRE 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. At the Government’s option, the Government will either place an order for a dedicated circuit data connection to be installed (within 60 calendar days) between the contractor's location(s) and SSA's network interface location or the connectivity method will be through the Internet using an encrypted VPN tunnel. The connection method is at the sole discretion of the Government. The Government shall not be responsible for installation delays of data connections due to any external influences such as employee strikes, weather, supplies, etc., which conditions are beyond the control of the Government.

If the Government selects a VPN Internet connection method, the contractor must have an Internet ready VPN IP security (IPsec) capable devise. The Government will not be responsible for any cost associated with the VPN Internet connection that the contractor may incur.

If the Government selects a dedicated circuit transmission, SSA will determine the appropriate bandwidth for the connection. The cost of this connection will be borne by the Government. The contractor shall immediately provide a complete delivery address with nearest cross street, contact name, and phone number for installation of data transmission services and equipment. The contact person at the contractor’s site will be available for delivery of services at the specified location. The Government shall not be responsible for incorrect or lack of address information, nor for non-availability of contact person at the delivery site. SSA will provide the necessary dedicated data connection, including a router, modem, and firewall at the contractors’ specified location(s).

The contractor shall provide adequate rack space for securing the router and firewall; the contractor shall provide a dedicated analog dial-up line within eight (8) feet of the router. This dedicated analog dial-up line will be used for router management and access for troubleshooting. The line must be in place and active prior to the installation of the circuit/router and equipment.

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

WIRE TRANSMISSION TEST: After the appropriate bandwidth data connection has been installed, the contractor will be required to receive within one (1) workday, data for 580,000 notices (multiple pages). The contractor will be required to perform a record count verification broken down by dataset name within one (1) workday after the complete transmission of the test files.

When the count verification has been successfully completed, the contractor will be required to provide SSA within five (5) workdays, 275 sample documents (25 notices from each of the eleven mailers. **Please note there is an exception to Mailers 1 through 4.** The samples will be produced using the data from each of the files that were transmitted during the wire transmission test. Samples may be imaged on white paper and contain only variable information or in PDF format. It will be at the discretion of SSA if one or both proofing methods will be used. Wire transmission test samples in paper format do not require inserts or envelopes.

** Wilkes-Barre Data Operations Center (WBDOC) will perform validation on the identical material for Mailers 1 through 4 on white paper imaged material only. The contractor must produce 50 press samples of each notice type on their equipment (that will be used in production), and with their personnel. The press samples are to be printed on the paper required by these specifications, trimmed, and folded. These press samples must be complete and include all variable fill-in information.

Submit all printed test samples to SSA, DPAMS, and/or WBDOC (see Exhibits).

NOTE: The wire transmission test will begin after the Government is notified of the availability of the system.

The Government will approve, conditionally approve, or disapprove the samples from the Wire Transmission Test within two (2) 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.

NOTE: If errors are found, 25 additional samples of each notice in error (Mailers 1 through 11) will be required until such time as the validation produces no errors.

SECURE FILE TRANSER PROTOCOLS (SFTP) SITE: Contractor is required to set up, establish, and maintain an SFTP 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.

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

SSA utilizes, and the contractor must provide compatibility with, Managed File Transfer (formerly known as Cyberfusion Integration Suite) software from TIBCO. The contractor may implement the Managed File Transfer Platform Server that has embedded software encryption capable of being enabled. The personal computers/servers must have the capability to run Managed File Transfer software with encryption enabled using IP protocols on Windows, UNIX (i.e., IBM’s AIX, SUN, or HP), or z/OS platforms.

SSA will not permit any private class A, B, or C IP addresses, i.e., 10.xxx.xxx.xxx type IP addresses from external users on its network. At connection time to SSA, the contractor will be provided a suitable IP address for access to SSA’s network via a firewall. SSA will provide the necessary subnet(s) for connection at the remote site. The contractor will be responsible for their own name/address translation to fulfill the intended purpose of data transfers. SSA will 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 the SSA will be written as Physical Sequential or “flat” files at the contractor’s location and will be distinguished with a “run date” in the contractor’s file name.

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

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

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

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

It is the contractor's responsibility to notify SSA in the event that any transmissions cannot be processed due to media problems, link problems or data transmission circuit/connection outages. The contractor shall immediately notify SSA's HELP DESK operations immediately (available 24/7) at (877) 697-4889 and report required observations and findings.

Transmission of production files shall 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.

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**.**

PROOFING AND TRANSMISSION/PRE-PREPRODUCTION VALIDATION TESTS: Prior to the commencement of production of orders placed under this contract, the Government will furnish electronic test files shortly after the postaward conference. The contractor will be required to demonstrate their ability to perform to the contract requirements by performing the following tests:

- Proofing for Initial Start-up
- Transmission Test
- Preproduction and Validation Test

Proofing for Initial Start-Up: The contractor must submit proofs for all scannable forms, personalized notices w/micro-perforated payment stub, instructions sheets, flyer, and envelopes under this contract within **seven (7) workdays** after receipt of furnished materials. Furnished materials (if manuscript or camera is provided) must be returned with proofs.

Prior to the commencement of production of orders placed under this contract, the contractor will be required to demonstrate their ability to perform the contract requirements. The Government will furnish electronic test files that are to be used in performing the Transmission Test and Pre-Production Validation Tests.

NOTE: Failure of the contractor to perform the Transmission Test and/or the Pre-Production Validation Tests to the satisfaction of the Government may be cause for default. The Government reserves the right to waive the requirements of any or all of these tests. The contractor will be notified at the Postaward Conference if any test(s) will be waived.

TRANSMISSION TEST: After the appropriate data connection has been installed, the contractor will be required to receive, within **one (1) workday**, data for approximately 375,000 notices (Mailers 1–11). The contractor will be required to perform a Record Count Verification and a Coding Accuracy Support System (CASS) certification within **one (1) workday** after the complete transmission of the test files. The contractor will be required to copy the files to their own system and e-mail T. Marshall-Vanzego at tracey.marshall-vanzego@ssa.gov with the exact counts received (broken down by dataset name), before proceeding with any other processing. SSA will respond within **one (1) workday** of receipt for verification.

The contractor will be required to run the test file through their CASS certification system to ensure there are no problems with the reading of the address file. The contractor will be required to report to SSA with the test results. 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 **three (3) workdays**, 10 sample documents from the Transmission Test for each file (Mailers 1 through 11) transmitted during the test. The samples will be produced using the data from each of the files that were transmitted during the transmission test. Samples may be imaged on white paper and contain only variable information. Transmission Test samples do not require inserts or envelopes. Submit the test samples to: SSA, T. Marshall-Vanzego, DPAMS, 1343 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401.

The Government will approve, conditionally approve, or disapprove the samples from the Transmission Test within **two (2) 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.

Note: If errors are found, additional samples will be required until the validation produces no errors.

PRE-PRODUCTION VALIDATION TESTS: Prior to commencement of production of orders placed under this contract, the Government will furnish electronic test files shortly after the postaward conference to be used in performing the Pre-Production Validation Tests.

NOTE: The contractor is required to complete all Pre-Production Validation Tests on the equipment they intend to use during live production and using their personnel.

NOTE: The Government will issue a print order for validation. Upon completion of all validation requirement the Contractor will be reimbursed for all applicable costs according to “SECTION 4 – SCHEDULE OF PRICES”.

QUALITY CONTROL SAMPLES: The contractor will be required to create two (2) quality control samples to be drawn from the production stream at the same time. For smaller quantities, the contractor-sampling rate must be adjusted as necessary to generate samples *in the middle* of each version. One sample will be drawn, inspected, and retained as part of the contractor quality assurance records. The second sample drawn for SSA will be packed with the remaining samples associated with each task order and shipped to the Social Security Administration, DPAMS (see Exhibits).

NEW WORKLOAD NOTE: If new workloads are required, press samples with variable data (validation) will be required prior to the commencement of production. The contractor will be required to furnish 200 press samples (English and Spanish) for each new workload. The contractor must produce these press samples on their equipment (that will be used in production), and with their personnel. The press samples are to be printed on the paper required by these specifications trimmed and folded. These press samples must be complete and include all variable fill-ins.

These press samples will incorporate all aspects of the program except inserting and mailing (i.e., printing, gathering, binding, folding, and preparing finished forms for the inserting operation), unless otherwise specified. These press samples are to be completed in accordance with contract requirements.

If any contractor's errors are serious enough in the opinion of the GPO to require revised samples of the press samples without variable data and/or the press samples with variable data, the revised samples are to be provided at no additional expense to the Government. No extra time can be allowed for this operation; such operations must be accomplished within the original production schedule allotted in the specifications.

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. 12 dated March 2011.

Government Paper Specification Standards No. 12 - http://www.gpo.gov/pdfs/customers/sfas/vol12/vol_12.pdf

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

Notices and Scannable Forms: White Offset Book, basis weight: 50 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60 with exception requiring compatibility with OCR.

Mail-Out Envelopes (6-1/4 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 Offset Book, basis weight: 60 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60.

CRM and BRM 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; or at contractor's option, White Offset Book, basis weight: 50 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60.

PRINTING/IMAGING: Contractor will be required to convert furnished data for either laser or ion deposition printing. All imaging/printing shall have a minimum resolution of 600 x 600 dpi. The notices and scannable forms contain both static text matter and variable data.

The Government reserves the right to make changes to the envelopes or the format(s)/text of the notices/scannable form 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 shall 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.

In the event that the agency makes changes to any or all of the mailing components, the agency will exhaust the current supply before requiring the contractor to begin using the updated components. The Government will not be required to purchase from the contractor the surplus/inventory of any component remaining on-hand in excess of what was authorized when an envelope or format/text change is implemented.

Notices/Scannable Forms: Print in black ink.

NOTE: Contractor shall be responsible for dating all notices. The date used is to be the date notices mailed.

Mail-Out, CRM and BRM Envelopes: Print face and back (after manufacture) in black ink. Printing shall be in accordance with the requirements for the style of envelope ordered. All printing shall comply with all applicable U.S. Postal Service regulations. The envelope shall accept printing without feathering or penetrating to the reverse side.

Print or tint all envelopes on the inside (back - before manufacture) in black ink (lining is acceptable). The contractor may use his own design but must guarantee that the product will ensure complete opacity and prevent show through of any material contained therein.

For the BRM and CRM return envelopes, the contractor is responsible for the placement of the Facing Identification Mark (FIM) and the IMB using the camera-ready positives provided (envelope) to comply with current USPS standards. Print FIMs and Intelligent Mail Barcodes using the camera-ready positive provided. The FIMs and Intelligent Mail Barcodes should be placed on the mailing piece according to the current U.S. Postal Service's Domestic Mail Manual, "Barcoded Mail pieces."

RECYCLED PAPER LOGO/LEGEND: The recycled paper logo/legend must be printed in black on each notice/scannable form and insert in the lower right hand corner on the face of the notice/scannable form.

The recycled paper English logo/legend must print in black ink on envelopes (if recycled paper is used) in the lower left hand corner on the seam side of the envelope. The Spanish logo/legend must print in the lower right hand corner on the seam side of the envelope.

CRITERIA FOR DATA IMAGING: All variable data fill-ins requirements for the Mid-Year Mailer, NCOA, Step Parent, and Fee Adjustment notice workloads should be extracted from the files utilizing the Record Specifications for each workload. (see Exhibits)

PDF417 (Portable Data File) 2-D BARCODES: A 2-D barcode will be required on all pages of all scannable forms, at least 1/4" margins (quiet zone) is required top, bottom, left, and right of each 2-D barcode. Minimum resolution of 300 dpi, with 4.41 code words per inch. Height is 1/2", plus or minus 1/16"; length/width is 1-1/4", plus or minus 1/16". Data columns are to be preceded and followed by the standard PDF417 stop/start patterns, left row indicator, and right row indicator. The 2-D barcodes to be imaged on the scannable forms should contain the following data elements:

Field Name	**Field Size**
Form Number	17
Page Number	2 (contractor to insert)
Print Date	7 (MMCCYY)
SSN	10
BIC	3
First Name	16
Middle Name	2
Last Name	21
DOE	5
FRA	5
Earnings	7
Selection Date	7
PSC	2
DOB	7
Starting Month	10 (ex. SEPTEMBER)

Language Indicator	1 (E for English and S for Spanish)
End Character	1
Applicant Suffix	4

Final record and block lengths to be provided at the postaward conference. The PDF417 2-D barcodes must be in accordance with the requirements of ANSIMH 10.8.3M, unless otherwise specified. All data elements contained in the barcode must begin in the specified positions. Data elements can be filled with blanks if necessary to begin the next element in the proper position.

PRODUCTION INSPECTION: Production inspection(s) may be required at the contractors /subcontractors' plant for the purpose of establishing that the receipt of transmitted files, the printing of pamphlets, leaflets, forms and/or envelopes, the imaging, dating of form inserts, collating, folding, inserting and mailing is 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: A production inspection(s) may be required at the contractor /subcontractor's plant, before production begins on any new workloads.**

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 make-ready 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.
The contractor must notify the GPO of the date and time the press sheet inspection can be performed. In order for proper arrangements to be made, notification must be given at least 72 hours prior to the inspection. Notify the U.S. Government Publishing Office (GPO), Quality Control for Procured Printing, Washington, DC 20401, at (202) 512-0542.

NOTE: A press sheet inspection(s) may be required, at the contractor's plant, before production begins on any new or existing workloads. At the Government's option, the press sheet inspection may be waived.

MARGINS: Margins will be indicated on print order, sample, or furnished copy. Follow manuscript copy for envelopes for notices/scannable forms and Summary Sheet for proper margins.

BINDING: All pages in the notice and scannable form are gathered in numerical sequence. They are to be nested together with all faces forward and folded from a flat size of 8-1/2 x 11 to 8-1/2 x 5-1/2, title out.

NOTE: All printing, folding, and insertion of the product are to be done by mechanical means. Fold variances that exceed plus or minus 1/16" shall be cause for rejection.

CONSTRUCTION: Mail-out Envelope: Envelope must be open side, with gummed fold-over flap for sealing and contain side seams or high cut diagonal seams. Flap is at the contractor's option but must meet all USPS requirements. Flap must be coated with suitable glue that will securely seal the envelope without adhering to contents, permit easy opening by the recipient, and not permit resealing of the envelope.

Face of envelope to contain a 1-1/2 x 4-1/4" die cut address window with slightly rounded corners. Die cut 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). The 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 poly-type, transparent, low-gloss material that must be clear of smudges, lines, and distortions. Poly-type material must be securely affixed to the inside of the envelope so as not to interfere with insertion of contents. Window material must meet the current USPS readability standards/requirements.

CRM and BRM Return Envelopes: Envelope must be open side, with gummed fold-over flap for sealing and contain side seams or high cut diagonal seams. Flap depth must be 1-1/2" and 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). Must contain a clear area security tint, approximately 3-1/2 x 5/8", behind barcode to ensure the readability of the bar code by the U.S. Postal Service's readability standards. The CRM return envelope must accommodate the two-part scannable forms with only those manufactured folds as specified above. All sizes may be adjusted slightly if end product is suitable for the intended usage.

NOTE: The Government reserves the right to make changes to the size and position of mail-out envelope window openings during the term of the contract to comply with the USPS new Intelligent Mail Barcode. Notification of a proposed change will be given sufficient time for the contractor to allow for the change and submit proofs to the Government. Therefore, the contractor should not preprint or maintain more than a 90-day surplus/inventory of any of the mail-out envelopes required on this contract. The Government shall not be required to purchase from the contractor the surplus/inventory of any of the mail-out envelopes remaining on hand in excess of what was authorized when an envelope change is implemented.

PACKAGING: Gather the appropriate number of leaves per notice, fold, and insert into mail-out envelope with recipient's name and address on first page facing out for visibility through window envelope. 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 with only one notice inserted into each envelope. When required, either reply envelope(s) are inserted behind the notice (when viewed from the window side of the envelope). When required, insert scannable form, instructions, either return envelope (s) behind the notice (when viewed from the window side of the envelope).

NOTE: It is the contractor's responsibility to ensure that the correct material for each mailer will be matched with notices and scannable form (which contain 2-D barcode with personalized data) for the same beneficiary and be inserted correctly into the envelope.

Pack suitably in shipping containers.

DISTRIBUTION:

F.O.B. Destination:

Notices: On the first order and any order that requires a significant change to the language, format, or appearance of a notice, deliver f.o.b. destination 30 complete sample copies of each type of notice, inserted into mail out envelopes. DO NOT SEAL ENVELOPES. Deliver samples to: SSA, DPAMS (see Exhibits).

CRM Return and BRM Return envelopes: On the first order and any order that requires a copy change, deliver f.o.b. destination ten (10) production samples of each to: SSA, MPPT (see Exhibits)

F.O.B. Contractor's City:

Mail balance of all orders f.o.b. contractor's city. The contractor is responsible for all costs incurred in transporting this product to the U.S. Postal Service facility.

The contractor is cautioned that the "Postage and Fees Paid" indicia may be used only for the purpose of mailing material produced under this contract.

All expenses incidental to picking up and returning materials, submitting proofs, or priors if they are needed, and furnishing sample copies must be borne by the contractor.

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 USPS in accordance with appropriate USPS rules and regulations, including the USPS Domestic Mail Manual, and Postal Bulletins on Automation Compatible First Class Domestic Mail (automated and non-automated) 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) Non-automation (Presorted); and (f) Non-automation (Single Piece).

Notices contain USPS Intelligent Mail Barcode full service option. The contractor will be required to comply with USPS requirements and place the IMB on the 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.

NOTE: To achieve automation USPS postal discounts, the contractor is required to either presort the notices prior to printing or sort the mail after the notices are inserted. The contractor must disclose how they will achieve maximum postage discounts as required in the contract. The contractor must disclose and demonstrate how they will achieve automation USPS postal discounts prior to award.
Addresses for these mailers will come from SSA's Master Beneficiary Record (MBR). SSA will provide a certificate indicating that within the last six (6) months the MBR addresses have been matched against USPS certified Coding Accuracy Support System (CASS) software. SSA will provide an NCOA certificate indicating that, within the last 95 calendar days, the MBR addresses have been processed by a licensed National Change of Address service vendor.

NATIONAL CHANGE-OF-ADDRESS AND CODING ACCURACY SUPPORT SYSTEM: Addresses for the Mid-Year Mailer Notices will come from SSA's MBR. SSA will provide a certificate indicating that, within the last 180 days, the addresses have been matched against USPS certified Coding Accuracy Support System (CASS) certified ZIP Code software. New CASS certificates will be provided to the Contractor as required by the USPS Domestic Mail Manual.

NOTE: The contractor is not to, at any time change the addresses supplied by SSA.

In addition, 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 Barcode and the top and bottom edges of the window.

All letters in a mailing must pass the “tap” test in order to obtain the maximum postal discounts for the 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.

USPS CERTIFIED MAIL: The domestic mail pieces included in these mailings may be required to be mailed using USPS Certified Mail. The contractor will prepare these mail pieces according to USPS regulations contained in the Domestic Mail Manual (DMM) under Section 503.3.0, Certified Mail. Notices associated with the certified mail file shall be inserted into envelopes and processed as certified mail. The contractor must place the current Postal Service Form 3800 (20 digit certified number and barcode) on the envelope.

NOTE: Permit imprint may not be used if the mailing is less than 200 pieces or pieces that are not identical. Instead, the mail must be metered.

MAILING DOCUMENTATION: The contractor shall provide SSA with complete copies of all documents used by USPS to verify and accept the mail (e.g., computer records of presort ZIP+4, barcode breakdown, press runs, etc.) including USPS 3607R and/or GPO’s Form 712 (Certificate of Conformance) noted with file date and mailer number. The contractor shall place the number that is on top of the GPO Form 712 (the number that starts with "A") in the space provided on the USPS mailing statements. If no space is provided on the mailing statement, place the number in the upper right margin of the mailing statement. The contractor will use Federal Agency Cost Code 276-00038 on all mailing documents.

Within three (3) workdays of completion of each print order, the contractor shall provide pdf copies of all mailing documentation and matching 100% Accountability Summary reports to; SSA, DPAMS. (see Exhibits)

Furnished material, proofs, and USPS validated copies of postal documentation must be delivered (via overnight carrier or PDF copies via email) to the SSA, DPAMS (see Exhibits).

Upon completion of this contract, the contractor must return all camera copy/PDF files made for each product to SSA, DPAMS (see Exhibits)

CERTIFIED MAIL: Special Notice Option (SNO) mail pieces included in these mailings will be required to be mailed using USPS Certified Mail. A receipt showing that the mail was accepted by the Post Office is a requirement for SNO mail. The contractor will prepare these mail pieces according to USPS regulations contained in the Domestic Mail Manual (DMM) under Section 503.3.0, Certified Mail.

INTERNATIONAL REGISTERED MAIL: Special Notice Option mail pieces included in these mailings will be required to be mailed using USPS International Registered Mail since Certified Mail cannot be used for foreign addresses. A receipt showing that the mail was accepted by the Post Office is a requirement for SNO mail. The contractor will prepare these mail pieces according to USPS regulations contained in the International Mail Manual (IMM) under Section 330, Registered Mail.

SCHEDULE: Adherence to this schedule must be maintained. Contractor must not start production of any job prior to receipt of the daily electronic task order or print order, as applicable.

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

The first print order for actual production will be issued in June 2017. For each option year exercised, the files for the Mid-Year Mailer notices will be provided for each mailing in or around the fourth week of every June through October.

Furnished production files will be transmitted for the Mid-Year Mailer (MYM) workload, as follows:

- Mailers 1 and 2 - Transmit in June with a second transmission to occur in August
- Mailers 3 and 4 – Transmit in August through October. Transmissions August through October will only include L9781-SM-SUP and L9781-SM-SUP-SP.

Upon receipt of the production files for the third, fourth, and fifth print orders for Mailers 1 through 4 the contractor will send 25 pdf sample copies of the output to SSA for approval. SSA will review the sample copies and provide an "OK TO PRINT" within 48 hours. The contractor must not print or mail these notices prior to receipt of an "OK TO PRINT".

Furnished production files will be transmitted for the National Change of Address workload, as follows:

- Mailers 5 and 6 – Transmits in the months of March, June, September, and December.

Furnished production files will be transmitted for the Step Parent workload, as follows:

- Mailers 7 through 9 - Transmits in December.

Furnished production files will be transmitted for the Fee Adjustment workload, as follows:

- Mailers 10 and 11 - Transmits in November.

NOTE: Any or all mailers can include certified or registered mail files. These specific files will mail only when required and will mail with any of the print orders. The contractor is to adhere to the corresponding mail schedule for the print order in which the certified mail files occur.

The contractor must notify the GPO of the date and time the press sheet inspection can be performed. In order for proper arrangements to be made, notification must be given at least 72 hours prior to the inspection. Notify the U.S. Government Publishing Office (GPO), Quality Control for Procured Printing, Washington, DC 20401, at (202) 512-0542. Telephone calls will only be accepted between the hours of 8:00 am and 2:00 pm, prevailing Eastern Standard Time (EST), Monday through Friday.

NOTE: See contract clauses, paragraph 14(e) (1), Inspections and Tests of GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987 (Rev. 6-01)).

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.

Proofs: The contractor must submit all proofs for the envelopes within seven (7) workdays after receipt of furnished materials. The Government will hold proofs no more than three (3) workdays from their receipt thereof until they are made available for pickup. The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time. The contractor must submit revised proofs, if necessary due to author's alterations, within three (3) workdays of notification. The Government will hold revised proofs for three (3) workdays from receipt thereof until made available for pickup.

For Press Samples with Variable Data (Validation):

The contractor shall submit the samples with the variable data within five (5) workdays after Government approval of proofs. The contractors shall furnish press samples with variable data in accordance with contract requirements. The Government will approve, conditionally approve, or disapprove the press samples with variable data validation output within five (5) workdays of receipt thereof. If necessary, the contractor must submit revised press samples with variable data within three (3) workdays of notification. The Government will approve, conditionally approve or disapprove the revised press samples without variable data within three (3) workdays of receipt thereof.

For Production and Mailing:

Contractor must provide SSA with notice counts within one (1) workday after receiving files to verify that complete files have been received. Contractor must complete all printing and mailing for all orders within 10 workdays after receipt of "OK to Print" on proofs.

ACCELERATED PRODUCTION SCHEDULE: On occasion, the SSA may require an order to be produced on an accelerated schedule. Accelerated orders will require complete production and mailing of the notices within 5 (five) workdays after receipt of "O.K. to Print on proofs". For work produced under the accelerated production schedule. The contractor will receive a "Premium Payment" of 15%. Premium payments, when authorized, will apply to all items except Item IV., "PAPER" in the "SCHEDULE OF PRICES."

NOTE: Failure of the contractor to deliver work at the time specified will result in disallowance of billing invoice premium payments that were anticipated and the contractor will not list such items on their voucher. Sample copies of notices and envelopes (with first order or whenever SSA makes a significant change), delivered to SSA on regular schedules, must be delivered within 10 workdays after completion of the order.

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 the 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 under this contract for a like period of time.

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

I.	(a) 85
	(b) 15
II.	(a) 11
	(b) 81,321
	(c) 21,775
	(d) 16,496
III.	(a) 52,793
	(b) 21,775
	(c) 16,496
IV.	(a) 21,775
V.	(a) 1

SECTION 4 - SCHEDULE OF PRICES

Bids offered are f.o.b. destination to Baltimore, MD and f.o.b. contractor's city for all mailing.

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) shall be entered if bidder intends to furnish individual items at no charge to the Government.

Bids submitted with NB (No Bid) 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 is 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 invoices submitted to the GPO shall be based on the most economical method of production.

Fractional parts of 100 will be prorated at the per-100 rate. Contractors billing invoices must be itemized in accordance with the line items in the SCHEDULE OF PRICES

I. COMPOSITION: Prices offered must include the cost of all operations and materials necessary in accordance with the terms of these specifications for the notices, scannable forms, eight (8) mail-out envelopes, six (6) CRM return envelopes, and one (1) BRM return envelope.

(a) Notices and Scannable Forms... per page .... $___________

(b) Envelopes .... per envelope .... $___________

II. PRINTING/IMAGING AND BINDING, AND CONSTRUCTION: Prices offered must include the cost of all materials and operations (including proofs, press samples and stock) necessary for the complete printing/imaging, binding, and construction of the product listed in accordance with these specifications.

(a) *Make ready/setup charge.. $___________

* Contractor will be allowed only one (1) make ready/setup charge per order. This combined charge shall include all materials and operations necessary to make-ready and/or setup the contractor’s equipment for that run. Invoices submitted with more than one make-ready/setup charge per order will be disallowed.

(b) Notices and Scannable forms: Printing in black ....per 100 pages .... $___________

(c) Mail-out Envelopes: Printing in black, including construction...........per 100 envelopes ... $___________

(d) CRM/BRM Envelopes: Printing in black, including construction.....per 100 envelopes..... $___________

____
(Initials)

III. PAPER: Payment for all paper supplied by the contractor under the terms of these specifications, as ordered on the individual print order, will be based on the net number of leaves furnished for the product(s) ordered in the applicable "Trim Size" group. The cost of any paper required for make-ready or running spoilage must be included in the prices offered.

Computation of the net number of leaves will be based on the following:

Notices and Scannable forms:	8-1/2 x 11"	A charge will be allowed for one page-size leaf.
Mail-out Envelopes:	6-1/8 x 9-1/2"	One leaf will be allowed for each envelope.
CRM/BRM Return Envelopes:	5-3/4 x 8-3/4"	One leaf will be allowed for each envelope.

Per 100 Leaves

(a) Notices/Scannable Form, White Offset (50 lb.)……………………………………………….$______________

(c) Mail-out Envelope w/ window, White (24 lb.) or White Offset Book, (60 lb.)………….. .$______________

(d) BRM/CRM Return Envelope, White Writing (20 lb.) or White Offset Book (50 lb.) ……$_____________

IV. INSERTING AND MAILING: Prices offered must include the cost of all required materials and operations necessary for the mailing of the notices/scannable form including cost of collating notices (single or multiple leaves) in proper sequence and folding to required size in accordance with these specifications, insertion of notice(s) and reply envelope (if required) into mail-out envelope and mailing in accordance with these specifications.

Per 100 Mailers

(a) Mailers 1 through 11: Inserting of required materials for each mailer. .... $___________

V. PRE-PRODUCTION TESTS: Price offered must include all costs incurred in performing the tests as specified in these specifications. These costs shall cover but are not limited to: machine time, personnel, all required materials, wire transmissions, films, electronic pre-press, plates, 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) Wire Transmission Test (per test)…………………………………………………….……$__________

(b) Pre-production Validation Test (per test) ……………………………………………........$__________

____
(Initials)

INSTRUCTIONS FOR BID SUBMISSION: Fill out “SECTION 4. – SCHEDULE OF PRICES,” initialing or signing each page in the space(s) provided. Submit two copies (original and one exact duplicate) of the “SCHEDULE OF PRICES” with two copies of the GPO Form 910 “BID” form. Do not enter bid prices on GPO Form 910; prices entered in the “SCHEDULE OF PRICES” will prevail.

Bidder ____

____
(City - State)

By ____
(Signature and title of person authorized to sign this bid)

____
(Person to be contacted) (Telephone Number)

EXHIBIT A

CONTRACTOR PERSONNEL SECURITY CERTIFICATION

Purpose: This form is used for contractor personnel to certify that they understand SSA's security and confidentiality requirements.

I understand the SSA security and confidentiality requirements and agree that:

1. I will follow all SSA rules of conduct and security policy/privacy rules/regulations.

2. I agree not to construct and maintain, for a period of time longer than required by the contract, any file containing SSA data unless explicitly agreed to by SSA in writing as part of the task documentation.

3. I agree to safeguard SSA information, whether electronic or hardcopy, in secured and locked containers during transportation.

4. I will use all computer software according to Federal copyright laws and licensing agreements.

5. I agree to keep confidential any third-party proprietary information, which may be entrusted, to me as part of the contract.

6. I will comply with systems security requirements contained in the SSA Systems Security Handbook.

7. I will not release or disclose any information subject to the Privacy Act of 1974, the Tax Return Act of 1976, SSA Regulation 1 and section 1106 of the Social Security Act to any unauthorized person.

8. I understand that disclosure of any information to parties not authorized by SSA may lead to criminal prosecution under Federal law.

-- -------------------------------------
Contractor Date

--- --------------------------------------
Contractor Employee Date

--- --------------------------------------
Contractor Employee Date

--- --------------------------------------
Contractor Employee Date

--- --------------------------------------
Contractor Employee Date

-- ---------------------------------------
Contractor Employee Date

-- ---------------------------------------
Contractor Employee Date

-- ---------------------------------------
Contractor Employee Date

-- ---------------------------------------
Contractor Employee Date

-- ---------------------------------------
Contractor Employee Date

-- ---------------------------------------
Contractor Employee Date

-- ---------------------------------------
Contractor Employee Date

-- ---------------------------------------
Contractor Employee Date

-- ---------------------------------------
Contractor Employee Date

-- ---------------------------------------
Contractor Employee Date

-- ---------------------------------------
Contractor Employee Date

-- ---------------------------------------
Contractor Employee Date

--   ---------------------------------------
Contractor Employee   Date

--   ---------------------------------------
Contractor Employee   Date

--   ---------------------------------------
Contractor Employee   Date

--   ---------------------------------------
Contractor Employee   Date

--   ---------------------------------------
Contractor Employee   Date

--   ---------------------------------------
Contractor Employee   Date

--   ---------------------------------------
Contractor Employee   Date

--   ---------------------------------------
Contractor Employee   Date

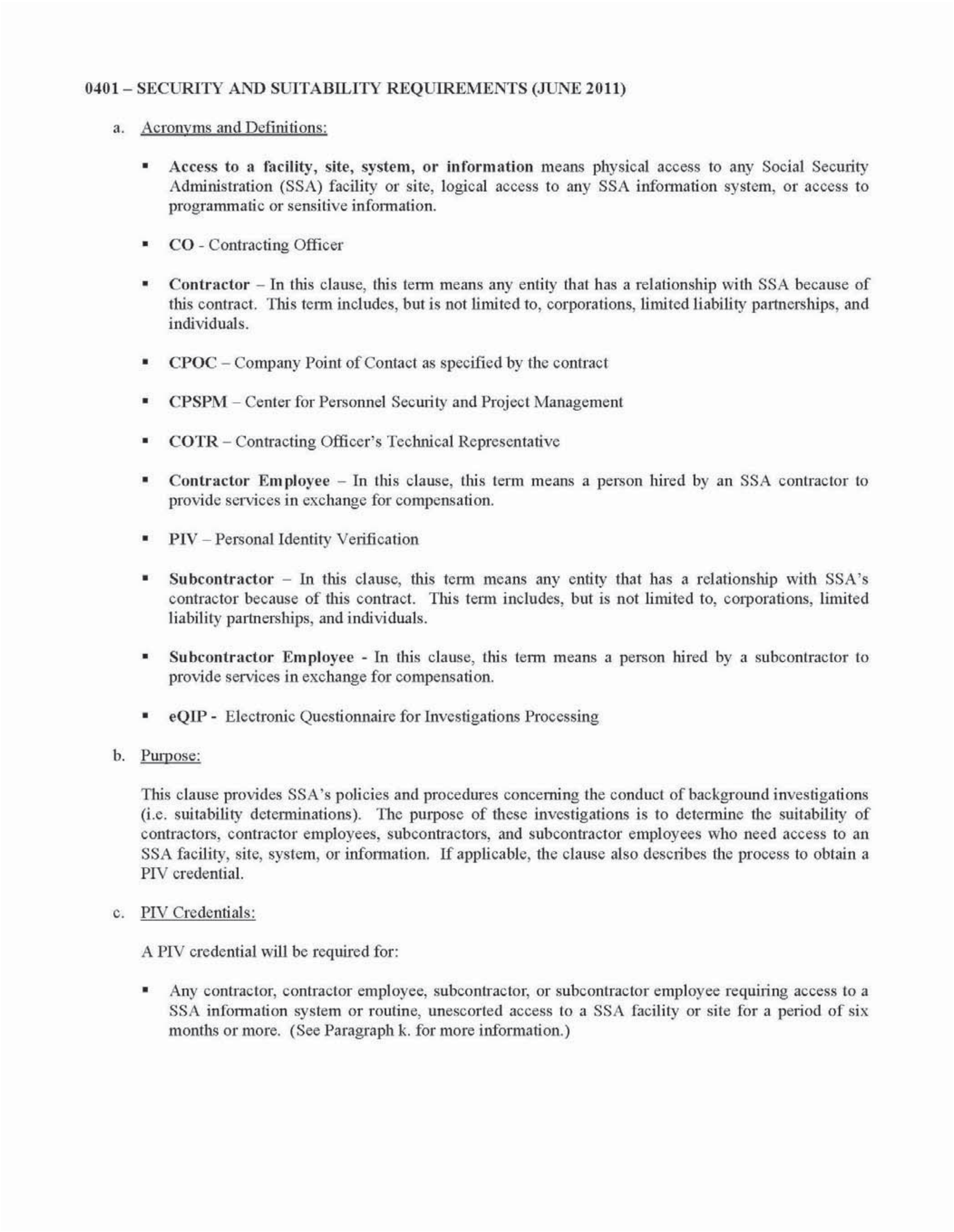
--   ---------------------------------------
Contractor Employee   Date

--   ---------------------------------------
Contractor Employee   Date

--   ---------------------------------------
Contractor Employee   Date

--   ---------------------------------------
Contractor Employee   Date

EXHIBIT B
Security and Suitability Requirements



0401 – SECURITY AND SUITABILITY REQUIREMENTS (JUNE 2011)

a. Acronyms and Definitions:

- **Access to a facility, site, system, or information** means physical access to any Social Security Administration (SSA) facility or site, logical access to any SSA information system, or access to programmatic or sensitive information.
- **CO** - Contracting Officer
- **Contractor** – In this clause, this term means any entity that has a relationship with SSA because of this contract. This term includes, but is not limited to, corporations, limited liability partnerships, and individuals.
- **CPOC** – Company Point of Contact as specified by the contract
- **CPSPM** – Center for Personnel Security and Project Management
- **COTR** – Contracting Officer's Technical Representative
- **Contractor Employee** – In this clause, this term means a person hired by an SSA contractor to provide services in exchange for compensation.
- **PIV** – Personal Identity Verification
- **Subcontractor** – In this clause, this term means any entity that has a relationship with SSA's contractor because of this contract. This term includes, but is not limited to, corporations, limited liability partnerships, and individuals.
- **Subcontractor Employee -** In this clause, this term means a person hired by a subcontractor to provide services in exchange for compensation.
- **eQIP -** Electronic Questionnaire for Investigations Processing

b. Purpose:

This clause provides SSA's policies and procedures concerning the conduct of background investigations (i.e. suitability determinations). The purpose of these investigations is to determine the suitability of contractors, contractor employees, subcontractors, and subcontractor employees who need access to an SSA facility, site, system, or information. If applicable, the clause also describes the process to obtain a PIV credential.

c. PIV Credentials:

A PIV credential will be required for:

- Any contractor, contractor employee, subcontractor, or subcontractor employee requiring access to a SSA information system or routine, unescorted access to a SSA facility or site for a period of six months or more. (See Paragraph k. for more information.)

A PIV credential will not be required for:

- Any contractor, contractor employee, subcontractor, or subcontractor employee requiring escorted access to a SSA facility or site for less than six months.

- Any contractor, contractor employee, subcontractor, or subcontractor employee requiring infrequent escorted access to a SSA facility or site, even if the access may be longer than six months. For example, contractors or contractor employees who provide infrequent facilities/equipment maintenance or repair, conduct onsite shredding, etc.

Please Note: A background investigation is required any time a contractor, contractor employee, subcontractor, or subcontractor employee requires any type of access to a facility, site, system, or information regardless of whether a credential is required or not.

The contractor is required to include the substance of this clause in any subcontract where subcontractors and subcontractor employees will have similar access as described in the preceding paragraphs. However, the contractor is responsible for obtaining all of the required forms (see paragraphs g-i) from its subcontractors and the subcontractors' employees, reviewing these forms, and submitting them to SSA. Subcontractors and subcontractors' employees shall not submit forms directly to SSA.

d. Authorities:

- Homeland Security Presidential Directive 12

- Office of Management and Budget Memorandum M-05-24

- The Crime Control Act of 1990, Public Law 101-647, subtitle E, as amended by Public Law 102-190 (for childcare center security requirements)

- Executive Orders 10450 and 12968 and Title 5, Code of Federal Regulations (CFR), Parts 731, 732 and 736 (for positions assigned a "National Security" designation)

e. Background Investigation and Adjudication Process:

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

f. Listing of Applicants:

Upon award, the CPOC will provide to SSA an applicant listing of **all** individuals for whom the contractor is requesting a suitability determination (i.e., background investigation). This listing should include the contractor's name, the contract number, the CPOC's name, the CPOC's contact information, each applicant's full name, each applicant's Social Security number (SSN), each applicant's date of birth, and each applicant's place of birth (must show city and state if born in the United States (U.S.) OR city and country if born outside of the U.S.). The background investigation process does not start until the CPOC submits this applicant listing; therefore, the CPOC should submit the listing as soon as practical after award.

Submit the applicant listing via U.S. Mail to the address located in paragraph i. OR via fax to 410-966-0640.

g. Required Forms:

1) eQIP:

SSA will initiate the eQIP process using the applicant listing provided by the CPOC. SSA will email notification to the CPOC that each applicant has been invited into the eQIP website to electronically complete their background investigation form. The CPOC will provide the website to the applicants to complete their eQIP form. The applicant will have up to seven (7) calendar days to complete the eQIP form. The 7-day timeframe begins once SSA notifies the CPOC of the eQIP invitation(s). The applicant must print the signature pages of the form (pages 5 and 6 for Standard Form (SF) 85; pages 7-9 for SF 85P), sign the signature pages, and then provide the signed originals to the CPOC.

2) Paper Forms:

- **Two (2) Field Division-258 charts, *Applicant Fingerprint Chart*** (The CO will provide the FD-258 charts at the time of contract award.)

  NOTE: The contractor will be responsible for obtaining and providing acceptable fingerprints for use by SSA. Regardless of the method used to fingerprint contractors, contractor employees, subcontractors, or subcontractor employees, (electronic capture or ink) the only acceptable fingerprint chart is the FD-258.

- **Optional Form 306, *Declaration for Federal Employment:***
  http://www.opm.gov/forms/html/of.asp

- **Fair Credit Reporting Act Authorization Form**
  Federal Investigations Notice: 98-02

- **Original signed and dated eQIP Signature Pages** (See paragraph g.1 above)

- **If the contractor, contractor employee, subcontractor or subcontractor employee is not a U.S. Citizen**, the individual must provide SSA with a legible photocopy of his or her work authorization permit and Social Security card.

h. Forms Completion:

The CPOC must ensure **all paper forms are fully completed and signed prior to submission to SSA.** The fingerprint charts and all paper forms must be legible or typed in black ink and all signatures must be in black ink. There must be no "breaks" in residences or employment. SSA requires complete addresses, including zip codes and phone numbers. SSA must receive forms within 30 days of signature and date.

SSA will return forms not fully completed to the CPOC. To ensure the forms are completed correctly, obtain a sample of a properly completed form at the following website: http://www.ssa.gov/oag/acq/Sample_Security_Requirement_Docs%20.pdf. Access information related to the eQIP process at: e-QIP - Quick Reference Guide for the Applicant.

i. Forms Submission:
j.

The CPOC shall submit **one cover sheet** to SSA containing the names of all of the individuals for whom the contractor is submitting completed paperwork. This cover sheet should include the contract number, each applicant's full name, each applicant's SSN, each applicant's date of birth, and each applicant's place of birth. Submit this cover sheet along with the completed paper forms and two FD-258 fingerprint charts for each applicant to:

SSA
CPSPM Suitability Team
6401 Security Boulevard
Room 1260 Dunleavy Building
Baltimore, MD 21235

Simultaneously, the CPOC must submit a copy of the cover sheet ONLY to the COTR.

The CPOC must submit the paper forms **at least 15 days prior to the date work is to begin.** For new contract employees, subcontractors, or subcontract employees (i.e., those who had not previously received a suitability determination under this contract) who will need access to a SSA facility, site, information, or system, the contractor must submit these forms at least 15 days prior to beginning work under the contract.

k. Suitability Determination:

A Federal Bureau of Investigation fingerprint check will be used 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 individual unsuitable to continue performing under this contract. CPSPM will notify the CPOC, COTR, and CO of the results of these determinations.

No contractor, contractor employee, subcontractor, or subcontractor employee will be allowed access to a SSA facility, site, information, or system until CPSPM has issued a favorable suitability determination for that contractor, contractor employee, subcontractor, or subcontractor employee.

A contractor is not entitled to an equitable adjustment of the contract because of an unfavorable suitability determination(s). Additionally, if SSA determines that the number or percentage of unfavorable determinations make successful contract performance unlikely, SSA may terminate the contract for cause or default.

The contractor must notify the contractor employee, subcontractor, or subcontractor employee of any unsuitable determinations as soon as possible after receipt of such a determination (see paragraph p., below, for an explanation of the appeals process).

l. Obtaining a Credential:

NOTE: This section applies only if the contractor, contractor employee, subcontractor, or subcontractor employee will have access to a facility, site, system, or information as described in the first bullet of paragraph c.

Once the contractor, contractor employee, subcontractor, or subcontract employee receives notification of an acceptable suitability determination, but prior to beginning work under the contract, the contractor, contractor employee, subcontractor, or subcontract employee must appear at the respective Regional Security Office or at SSA Headquarters Parking and Credentialing Office to begin the credentialing process. The contractor, contractor employee, subcontractor, or subcontract employee must present the suitability determination letter and two forms of identification at this meeting. At least one of the forms of identification must be a Government-issued photo identification (ID) (please see Employment Eligibility Verification, I-9, for acceptable forms of ID). For SSA Headquarters access, a completed Form SSA-4395, Application for Access to SSA Facilities, signed by the contractor, contractor employee, subcontractor, or subcontract employee and the COTR is also required. The COTR will provide the SSA-4395 Form to the contractor, contractor employee, subcontractor, or subcontract employee when applicable.

The contractor must contact the COTR to arrange for credentialing. The COTR is responsible for scheduling an appointment for contractors, contractor employees, subcontractors, or subcontract employees to meet with the appropriate SSA Parking and Credentialing Office or Regional Security Office and obtain a credential. Once the COTR makes the appointment, the COTR must contact the contractor to inform the contractor of the credentialing appointment(s). The COTR must also arrange for the contractor, contractor employees, subcontractors, or subcontract employees to be escorted (by either the COTR or a COTR's representative) to the appropriate credentialing office at the time of this appointment.

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

SSA Headquarters' Parking and Credentialing Office representatives can be reached by emailing Parking.and.Credentialing@ssa.gov or calling 410/965-5910.

Regional Security Office contact information can be found in the Appendix at the end of this clause.

m. Contractors, Contractor Employees, Subcontractors, or Subcontract Employees Previously Cleared by SSA or Another Federal Agency:

If a contractor, contractor employee, subcontractor, or subcontract employee previously received a suitability determination from SSA or another Federal agency, the CPOC should include this information next to the individual's name on the initial applicant listing (see paragraph f.). CPSPM will review the information. If CPSPM determines another suitability determination is not required, it will provide a letter to the CPOC and COTR indicating the contractor, contractor employee, subcontractor, or subcontract employee was previously cleared under another Federal contract and does not need to go through the suitability determination process again.

n. Contractor Notification to Government:

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

o. Contractor Return of PIV Credential:

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

p. Government Control:

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

q. Appeals Process for Unsuitable Determinations:

If a contractor, contractor employee, subcontractor, or subcontract employee would like clarification or wishes to appeal an unsuitable determination, his/her request must be in writing and submitted within 30 days of the date of the unsuitable determination. The contractor may not file appeals on behalf of its employees, subcontractors, or subcontract employees; rather, contractor employees, subcontractors, or subcontract employees must file their own individual appeals.

The request for clarification and/or the appeal can be emailed to SSA at: dchr.ope.hspd12appeals@ssa.gov, or mailed to:

Social Security Administration
Attn: CPSPM Suitability Program Officer
6401 Security Boulevard
Room 1260 Dunleavy Building
Baltimore, MD 21235

r. Removal From Duty:

SSA may remove a contractor, or request that the contractor immediately remove or cause to be removed any contractor employee, subcontractor, or subcontract employee from working under the contract based on conduct that occurs after a favorable suitability determination. This includes temporarily removing a contract employee, subcontractor, or subcontract employee should the individual be arrested for a violation of law pending the outcome of any judicial proceedings. The contractor must comply with these requests to remove or cause to have removed any contractor employee, subcontractor, or subcontract employee. The Government's determination may be made based on, but not limited to, incidents involving the misconduct or delinquency as set forth below:

i. Violation of the Rules and Regulations Governing Public Buildings and Grounds, 41 CFR 101-20.3. This includes any local badging requirements.

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

iii. Falsification or unlawful concealment, removal, mutilation, or destruction of any official documents or records, or concealment of material facts by willful omissions from official documents or records.

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

v. Theft, vandalism, or any other criminal actions.

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

vii. Improper use of official authority or credentials.

viii. Unauthorized use of communications equipment or Government property.

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

x. Unauthorized access to areas not required for the performance of the contract.

xi. Unauthorized access to employees' personal property.

xii. Violation of security procedures or regulations.

xiii. Prior determination by SSA or other Federal agency that a contractor, contractor employee, subcontractor, or subcontract employee was unsuitable.

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

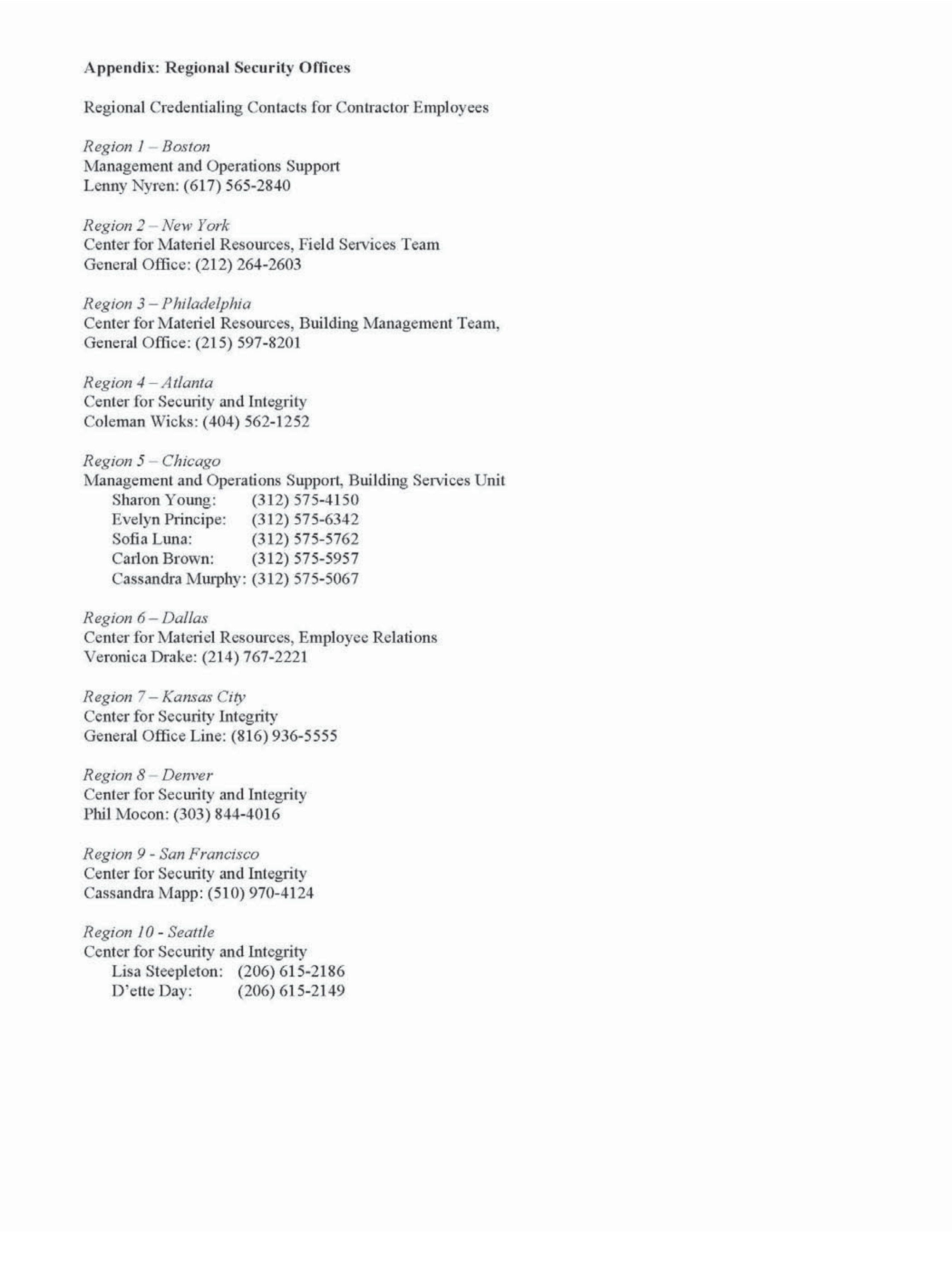
xv. Unauthorized access to an agency Automated Information System.

xvi. Unauthorized access of information for personal gain (including, but not limited to, monetary gain), or with malicious intent.

xvii. Not providing for the confidentiality of and protection from disclosure of information entrusted to them. Certain provisions of the following statutes and regulations that apply to Federal employees also apply equally to contractors, contractor employees, subcontractors, and subcontract employees:

- The Privacy Act of 1974
- The Tax Reform Act of 1976 and the Taxpayer Browsing Protection Act of 1997
- SSA regulation 1
- The Computer Fraud and Abuse Act of 1986
- Section 1106 of the Social Security Act

xviii. Being under investigation by an appropriate authority for violating any of the above.



Appendix: Regional Security Offices

Regional Credentialing Contacts for Contractor Employees

Region 1 – Boston
Management and Operations Support
Lenny Nyren: (617) 565-2840

Region 2 – New York
Center for Materiel Resources, Field Services Team
General Office: (212) 264-2603

Region 3 – Philadelphia
Center for Materiel Resources, Building Management Team,
General Office: (215) 597-8201

Region 4 – Atlanta
Center for Security and Integrity
Coleman Wicks: (404) 562-1252

Region 5 – Chicago
Management and Operations Support, Building Services Unit

Sharon Young:	(312) 575-4150
Evelyn Principe:	(312) 575-6342
Sofia Luna:	(312) 575-5762
Carlon Brown:	(312) 575-5957
Cassandra Murphy:	(312) 575-5067

Region 6 – Dallas
Center for Materiel Resources, Employee Relations
Veronica Drake: (214) 767-2221

Region 7 – Kansas City
Center for Security Integrity
General Office Line: (816) 936-5555

Region 8 – Denver
Center for Security and Integrity
Phil Mocon: (303) 844-4016

Region 9 - San Francisco
Center for Security and Integrity
Cassandra Mapp: (510) 970-4124

Region 10 - Seattle
Center for Security and Integrity

Lisa Steepleton:	(206) 615-2186
D'ette Day:	(206) 615-2149

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	□ None □ NPRC □ At SON	Other Address	ZIP Code
L SOI		M Location of Security Folder	□ None □ At SOI □ NPI	Other Address	ZIP Code

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.

4 SOCIAL SECURITY NUMBER

City	County	State	Country *(if not in the United States)*	

5 OTHER NAMES USED

#1	Name	Month/Year To Month/Year	#3	Name	Month/Year To Month/Year
#2	Name	Month/Year To Month/Year	#4	Name	Month/Year To Month/Year

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)* □ Day □ Night ( )	Home *(include Area Code)* □ 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.*	b Your Mother's Maiden Name
	□ 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.*	

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.

Month/Year Month/Year #1 To Present	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 Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor

Month/Year Month/Year #2 To	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 Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor

Month/Year Month/Year #3 To	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 Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor

Enter your Social Security Number before going to the next page →

YOUR EMPLOYMENT ACTIVITIES *(CONTINUED)*

#4 Month/Year Month/Year To	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank

Employer's/Verifier's Street Address	City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)	City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)	City (Country)	State	ZIP Code	Telephone Number ( )

PREVIOUS PERIODS OF ACTIVITY *(Block #4)*	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor

#5 Month/Year Month/Year To	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank

Employer's/Verifier's Street Address	City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)	City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)	City (Country)	State	ZIP Code	Telephone Number ( )

PREVIOUS PERIODS OF ACTIVITY *(Block #5)*	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor

#6 Month/Year Month/Year To	Code	Employer/Verifier Name/Military Duty Location	Your Position Title/Military Rank

Employer's/Verifier's Street Address	City (Country)	State	ZIP Code	Telephone Number ( )
Street Address of Job Location (if different than Employer's Address)	City (Country)	State	ZIP Code	Telephone Number ( )
Supervisor's Name & Street Address (if different than Job Location)	City (Country)	State	ZIP Code	Telephone Number ( )

PREVIOUS PERIODS OF ACTIVITY *(Block #6)*	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor
	Month/Year Month/Year To	Position Title	Supervisor

12 YOUR EMPLOYMENT RECORD	Yes	No
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.		

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 #1	Dates Known Month/Year To Month/Year	Telephone Number □ Day □ Night ( )		
Home or Work Address	City (Country)		State	ZIP Code

Name #2	Dates Known Month/Year To Month/Year	Telephone Number □ Day □ Night ( )		
Home or Work Address	City (Country)		State	ZIP Code

Name #3	Dates Known Month/Year To Month/Year	Telephone Number □ Day □ Night ( )		
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)*	3 - Stepmother	5 - Foster Parent	7 - Stepchild
2 - Father *(second)*	4 - Stepfather	6 - Child *(adopted also)*	

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.)*

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.

Yes	No

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**

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?

	Yes	No
a		
b		

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	Controlled Substance/Prescription Drug Used	Number of Times Used
To		
To		
To		

22 **YOUR FINANCIAL RECORD**

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.

Yes	No

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.

If you answered "**Yes,**" provide the information requested below:

Yes	No

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 D - Fingerprint Card

APPLICANT
* See Privacy Act Notice on Back

FD-258 (REV.12-10-07)

LEAVE BLANK

TYPE OR PRINT ALL INFORMATION IN BLACK

LAST NAME NAM FIRST NAME MIDDLE NAME

FBI LEAVE BLANK

SIGNATURE OF PERSON FINGERPRINTED

R
I

RESIDENCE OF PERSON FINGERPRINTED

DATE OF BIRTH DOB
Month Day Year

CITIZENSHIP CTZ	SEX	RACE	HGT.	WGT.	EYES	HAIR

PLACE OF BIRTH POB

DATE

SIGNATURE OF OFFICIAL TAKING FINGERPRINTS

EMPLOYER AND ADDRESS

REASON FINGERPRINTED

YOUR NO. OCA

FBI NO. FBI

ARMED FORCES NO. MNU

SOCIAL SECURITY NO. SOC

MISCELLANEOUS NO. MNU

LEAVE BLANK

CLASS

REF.

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

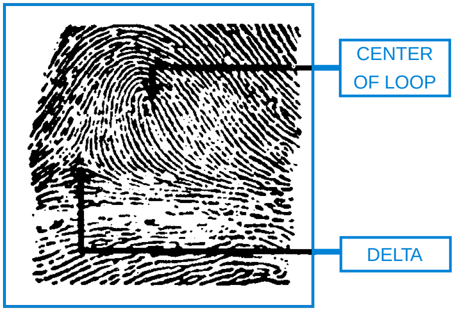
Exhibit F: Fingerprint Card

1110-0046 3/21/2010

FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE
CJIS DIVISION/CLARKSBURG, WV 26306

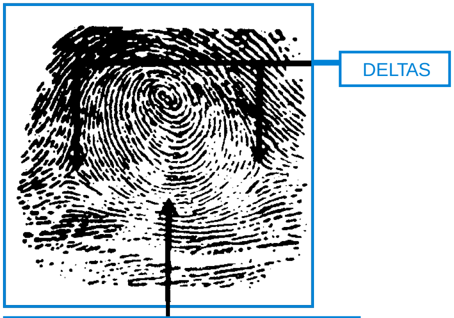
APPLICANT

1. LOOP



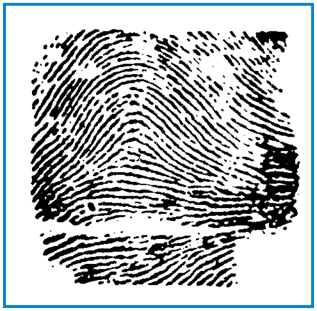
THE LINES BETWEEN CENTER OF LOOP AND DELTA MUST SHOW

2. WHORL



THESE LINES RUNNING BETWEEN DELTAS MUST BE CLEAR

3. ARCH



ARCHES HAVE NO DELTAS

FD-258 (REV. 12-10-07)

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 STSTES. 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 criminal and 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.)

•'b7 The required fields for hard copy fingerprint cards are: originating agency identifier number - date of birth - place of birth - name - sex fingerprint impressions - any applicable state stamp - Other (race, height, weight, eye color, hair color)

* criminal fingerprint cards also require an arrest charge and date of arrest.
* civil fingerprint cards also require a reason fingerprinted and date fingerprinted

Do not use highlighters on fingerprint cards.
Do not enter data or labels within 'Leave Blank' areas.
Ensure the 'Reply Desired' field is checked when applicable (criminal only**).**
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 Identification and Investigative Services Section's Customer Service Group at (304) 625-5590 or by e-mail at <liaison@leo.gov>.

PRIVACY ACT STATEMENT

Authority: The FBI's acquisition, preservation, and exchange of information requested by this form is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include numerous Federal statutes, hundreds of State statutes pursuant to Pub.L. 92-544, Presidential executive orders, regulations and/or orders of the Attorney General of the United States, or other authorized authorities. Examples include, but are not limited to: 5 U.S.C. 9101; Pub.L. 94-29; Pub.L. 101-604; and Executive Orders 10450 and 12968. Providing the requested information is voluntary; however, failure to furnish the information may affect timely completion or approval of your application.

Social Security Account Number (SSAN). Your SSAN is needed to keep records accurate because other people may have the same name and birth date. Pursuant to the Federal Privacy Act of 1974 (5 USC 552a), the requesting agency is responsible for informing you whether disclosure is mandatory or voluntary, by what statutory or other authority your SSAN is solicited, and what uses will be made of it. Executive Order 9397 also asks Federal agencies to use this number to help identify individuals in agency records.

Principal Purpose: Certain determinations, such as employment, security, licensing, and adoption, may be predicated on fingerprint-based checks. Your fingerprints and other information contained on (and along with) this form may be submitted to the requesting agency, the agency conducting the application investigation, and/or FBI for the purpose of comparing the submitted information to available records in order to identify other information that may be pertinent to the application. During the processing of this application, and for as long hereafter as may be relevant to the activity for which this application is being submitted, the FBI may disclose any potentially pertinent information to the requesting agency and/or to the agency conducting the investigation. The FBI may also retain the submitted information in the FBI's permanent collection of fingerprints and related information, where it will be subject to comparisons against other submissions received by the FBI. Depending on the nature of your application, the requesting agency and/or the agency conducting the application investigation may also retain the fingerprints and other submitted information for other authorized purposes of such agency(ies).

Routine Uses: The fingerprints and information reported on this form may be disclosed pursuant to your consent, and may also be disclosed by the FBI without your consent as permitted by the Federal Privacy Act of 1974 (5 USC 552a(b)) and all applicable routine uses as may be published at any time in the Federal Register, including the routine uses for the FBI Fingerprint Identification Records System (Justice/FBI-009) and the FBI's Blanket Routine Uses (Justice/FBI-BRU). Routine uses include, but are not limited to, disclosures to: appropriate governmental authorities responsible for civil or criminal law enforcement, counterintelligence, national security or public safety matters to which the information may be relevant; to State and local governmental agencies and nongovernmental entities for application processing as authorized by Federal and State legislation, executive order, or regulation, including employment, security, licensing, and adoption checks; and as otherwise authorized by law, treaty, executive order, regulation, or other lawful authority. If other agencies are involved in processing this application, they may have additional routine uses.

Additional Information: The requesting agency and/or the agency conducting the application-investigation will provide you additional information pertinent to the specific circumstances of this application, which may include identification of other authorities, purposes, uses, and consequences of not providing requested information. In addition, any such agency in the Federal Executive Branch has also published notice

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.

3. FBI NUMBER, IF KNOWN, SHOULD ALWAYS BE FURNISHED IN THE APPROPRIATE SPACE.

** 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).

Form Approved:
OMB No. 3206-0182

Declaration for Federal Employment*

(*This form may also be used to assess fitness for federal contract employment)

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.

Form Approved:
OMB No. 3206-0182

Declaration for Federal Employment*

(*This form may also be used to assess fitness for federal contract employment)

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?**

□ YES □ NO (If "NO", provide country of citizenship) ♦

4. **DATE OF BIRTH** (MM / DD / YYYY)

♦

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*

Form Approved:
OMB No. 3206-0182

(*This form may also be used to assess fitness for federal contract employment)

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: ______________________ Date __________
(Sign in ink)

17b. Appointee's Signature: ______________________ Date __________
(Sign in ink)

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

Federal Investigations Notice

Letter No. 98-02
Date: March 6, 1998

On September 30, 1997, amendments to the Fair Credit Reporting Act (FCRA) (15 U.S.C. § 1681, *et seq.)* became effective as a result of the Consumer Credit Reporting Reform Act of 1996. The amendments require changes on the part of the users of consumer reports and providers of information to consumer reporting agencies. These changes impact on OPM-IS as the provider of investigative services to other Federal agencies, and on our customer agencies as the final users of credit information gathered as a result of OPM's investigations.

Most notably, **Section 1681b** of title 15 addresses permissible purposes for which consumer reports may be furnished and conditions for furnishing and using consumer reports for employment purposes. If an a enc. intends to use a consumer report for employment purposes, **Subsection 1681b (b) (2)** of title 15 requires that the applicant/employee be notified in a document consisting solely of the notice that a consumer report may be used, and the applicant/employee must authorize this use in writing before the consumer report is obtained. **Subsection 1681b (b)(3)** of title 15 requires that, before taking adverse action relative to an employment decision based on a consumer report, the agency must provide the consumer with a copy of the report, and a copy of the Federal Trade Commission's (FTC) Consumer Rights Notice.

The notice, disclosure, certification and adverse action requirements of the **FCRA** do not directly apply to OPM-IS in its role as the provider of investigative services to other requesting Federal agencies. However, we do obtain credit reports on behalf of other Federal agencies, and will require those Federal agencies to certify that they are the procurer of the credit report and that they are compliant with the FCRA's relevant provisions. We are, therefore, sending under separate cover a request to each agency for a one-time blanket certification to this effect, to be completed and returned to OPM-IS no later than May 1, 1998.

We will ask that the certification acknowledge that the requesting Federal agency is the procurer of the credit report for purposes of compliance with the FCRA. We will also ask that the requesting Federal agency certify that it is compliant with all relevant provisions of the FCRA. This certification should include certification that the agency will (a) clearly and conspicuously disclose to the subject of investigation, in a written document consisting solely of the disclosure, that the agency may obtain a credit report for employment purposes; and (b) obtain the subject's written authorization to obtain the credit report. It will also state that the agency will not take adverse action against the subject of investigation, based in whole or in part upon the credit report, without first providing the subject a copy of the report and a written description of the subject's rights as described by the FTC under **Section 1681g(c)(3)** of title 15. Finally, the certification must state that the requesting Federal agency will not use any information from the consumer report in violation of any applicable equal employment opportunity law or regulation.

A sample release for obtaining written authorization from each affected applicant/employee, as well as a copy of the FTC's Consumer Rights Notice are attached for your information and may be reproduced as necessary. You can obtain additional information regarding the FCRA at the Federal Trade Commission's web site (http://www.ftc.gov).

Attachments

Inquiries: OPM-IS, Oversight and Technical Assistance Division, 202-606-1042
OPM-FIPC, Contract Management Branch, 724-794-5612
Code:736
Distribution: SOI/SON's
Letter Expires: When superseded

SAMPLE RELEASE

Fair Credit Reporting Act of 1970, as amended

PLEASE TAKE NOTICE THAT ONE OR MORE CONSUMER CREDIT REPORTS MAY BE OBTAINED FOR EMPLOYMENT PURPOSES PURSUANT TO THE FAIR CREDIT REPORTING ACT, AS AMENDED, 15 U. S. C., §1681, ET SEQ. SHOULD A DECISION TO TAKE ANY ADVERSE ACTION AGAINST YOU BE MADE, BASED EITHER IN WHOLE OR IN PART ON THE CONSUMER CREDIT REPORT, THE CONSUMER REPORTING AGENCY THAT PROVIDED THE REPORT PLAYED NO ROLE IN THE AGENCY'S DECISION TO TAKE SUCH ADVERSE ACTION.

Information provided by you on this form will be furnished to the consumer reporting agency in order to obtain information in connection with an investigation to determine your (1) fitness for Federal employment, (2) clearance to perform contractual service for the Federal Government, and/or (3) security clearance or access. The information obtained may be redisclosed to other Federal agencies for the above purposes and in fulfillment of official responsibilities to the extent that such disclosure is permitted by law.

I hereby authorize the ______________________________ to obtain such report(s) from any
(Name of Requesting Agency)
consumer/credit reporting agency for employment purposes.

____________________ (Print Name)	________________________ (SSN)
____________________ (Signature)	________________________ (Date)

Your Social Security Number is needed to keep records accurate, because other people may have the same name. Executive Order 9397 also asks Federal agencies to use this number to help identify individuals in agency records.

A Summary of Your Rights Under the Fair Credit Reporting Act

The federal Fair Credit Reporting Act (FCRA) is designed to promote accuracy, fairness, and privacy of information in the files of every "consumer reporting agency" (CRA). Most CRAs are credit bureaus that gather and sell information about you -- such as if you pay your bills on time or have filed bankruptcy -- to creditors, employers, landlords, and other businesses. You can find the complete text of the FCRA, 15 U.S. C. 1681-168 1 u, at the Federal Trade Commission's web site (http:www.FTC.GOV). The FCRA gives you specific rights, as outlined below. You may have additional rights under state law. You may contact a state or local consumer protection agency or a state attorney general to learn those rights.

- You must be told if information in your file has been used against you. Anyone who uses information from a CRA to take action against you -- such as denying an application for credit, insurance, or employment -- must tell you, and give you the name, address, and phone number of the CRA that provided the consumer report.
- You can find out what is in your file. At your request, a CRA must give you the information in your file, and a list of everyone who has requested it recently. There is no charge for the report if a person has taken action against you because of information supplied by the CRA, if you request the report within 60 days of receiving notice of the action. You also are entitled to one free report every twelve months upon request if you certify that (1) you are unemployed and plan to seek employment within 60 days, (2) you are on welfare, or (3) your report is inaccurate due to fraud. Otherwise, a CRA may charge you up to eight dollars.
- You can dispute inaccurate information with the CRA. If you tell a CRA that your file contains inaccurate information, the CRA must investigate the items (usually within 30 days) by presenting to its information source all relevant evidence you submit, unless your dispute is frivolous. The source must review your evidence and report its findings to the CRA. (The source also must advise national CRAs -- to which it has provided the data -- of any error.) The CRA must give you a written report of the investigation, and a copy of your report if the investigation results in any change. If the CRA's investigation does not resolve the dispute, you may add a brief statement to your file. The CRA must normally include a summary of your statement in future reports. If an item is deleted or a dispute statement is filed, you may ask that anyone who has recently received your report be notified of the change.
- Inaccurate information must be corrected or deleted. A CRA must remove or correct inaccurate or unverified information from its files, usually within 30 days after you dispute it. However, the CRA is not required to remove accurate data from your file unless it is outdated (as described below) or cannot be verified. If your dispute results in any change to your report, the CRA cannot reinsert into your file a disputed item unless the information source verifies its accuracy and completeness. In addition, the CRA must give you a written notice telling you it has reinserted the item. The notice must include the name, address and phone number of the information source.
- You can dispute inaccurate items with the source of the information. If you tell anyone -- such as a creditor who reports to a CRA -- that you dispute an item, they may not then report the information to a CRAwithout including a notice of your dispute. In addition, once you've notified the source of the error in writing, it may not continue to report the information if it is, in fact, an error.
- Outdated information may not be reported. In most cases, a CRA may not report negative information that is more than seven years old; ten years for bankruptcies.
- Access to your file is limited. A CRA may provide information about you only to people with a need recognized by the FCRA -- usually to consider an application with a creditor, insurer, employer, landlord, or other business.
- Your consent is required for reports that are provided to employers, or reports that contain medical information. A CRA may not give out information about you to your employer, or prospective employer, without your written consent. A CRA may not report medical information about you to creditors, insurers, or employers, without your permission.
- You may choose to exclude your name from CRA lists for unsolicited credit and insurance offers. Creditors and insurers may use file information as the basis for sending you unsolicited offers of credit or insurance. Such offers must include a toll-free phone number for you to call if you want your name and address removed from future lists. If you call, you must be kept off the lists for two years. If you request, complete, and return the CRA form provided for this purpose, you must be taken off the lists indefinitely.

- You may seek damages from violators. If a CRA, a user or (in some cases) a provider of CRA data, violates the FCRA, you may sue them in state or federal court.

The FCRA gives several different federal agencies authority to enforce the FCRA:

FOR QUESTIONS OR CONCERNS REGARDING:	**PLEASE CONTACT:**
CRA's creditors and others not listed below	Federal Trade Commission Consumer Response Center-FCRA Washington , DC 20580 202-326-3761
National banks, Federal branches/agencies of foreign banks (word "National" or initials "N.A" appear in or after banks name)	Office of the Comptroller of the Currency Compliance Management Mail Stop 6-6 Washington , DC 20219 800-613-6743
Federal Reserve System member banks (except national banks, and Federal branches/agencies of foreign banks)	Federal Reserve Board Division of Consumer & Community Affairs Washington, DC 20551 202-452-3693
Savings associations and federally chartered savings banks (word "Federal or initials "F.S.B." appear in federal institutions name"	Office of Thrift Supervision Consumer Programs Washington, DC 20552 800-842-6929
Federal credit unions (words "Federal Credit Union" appear in institution's name)	National Credit Union Administration 1775 Duke Street Alexandria VA 22314 703-518-6360
State chartered banks that are not members of the Federal Reserve System	Federal Deposit Insurance Corp. Div. of Compliance & Consumer Affairs Washington, DC 20429 202-934-FDIC
Air, surface, or rail common carriers regulated by former Civil Aeronautics Board of Interstate Commerce Commission	Department of Transportation Office of Financial Management Washington, DC 20590 202-366-1306
Activities subject to the Packers and Stockyards Act, 1921	Department of the Agriculture Office of Deputy Administrator-GIPSA Washington, DC 20250 202-720-7051

[Enter Company/ Agency Name]

Security Categorization: [Enter Categorization]

SYSTEM SECURITY PLAN (SSP)

For

<Externally Hosted Information System Name>

<Information System Acronym>

< Version #. #>

<Date>

Prepared by

[Insert Company/Agency Logo]

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 that the system provides services for.

[Note: This SSP template is intended to be used to document an external hosted Information Systems that is NOT 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)**

Agreed: ______________________________ ________________
[ENTER NAME OF SO] ← DELETE Date
SSA System Owner

Agreed: ______________________________ ________________
[ENTER NAME OF ISSO] ← DELETE Date
(Hosting Company/Agency) Information System Security Officer

Agreed: ______________________________ ________________
[ENTER NAME OF SAM ← DELETE Date
SSA Security Authorization Manager

Agreed: ______________________________ ________________
[ENTER NAME OF AO] ← DELETE Date
SSA Authorizing Official (optional)

[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 impacting 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 TABLES

LIST OF FIGURES

1 INFORMATION SYSTEM IDENTIFICATION

1.1 INFORMATION SYSTEM NAME/TITLE

Table 1: System Name/Identifier

System Name/Title:	System ID No:
<External 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 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] ← DELETE THESE INSTRUCTIONS UPON COMPLETION

TABLE 4: INFORMATION DATA 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

TABLE 5: AUTHORIZING OFFICIAL (AO)

Name:	
Title:	
Agency:	
Address:	
Telephone:	
Email:	
Responsibility:	The Authorizing Official has the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Security Authorization Manager

Table 6: Hosting Contractor/Agency Information System Security Officer (ISSO)

Name:	
Title:	
Agency:	
Address:	
Telephone:	
Email:	

Responsibility:	Information System Security Officer

Table 7: System Owner (SO)

Name:	
Title:	
Agency:	
Address:	
Telephone:	
Email:	
Responsibility:	The System Owner is responsible for defining the application's operating parameters, authorized functions, and security requirements.

Table 8: SSA Security Authorization Manager (SAM)

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

Table 9: ADDITIONAL POCS (e.g. Subject Matter EXPERT, SSA Project Manager, etc...)

Name:	
Title:	
Agency:	
Address:	
Telephone:	
Email:	
Responsibility:	[Company Name] [Role]

[NOTE: Add additional contacts if necessary]← Delete

Table 10: Additional Designated Contacts

Name:	
Title:	
Agency:	
Address:	
Telephone:	
Email:	
Responsibility:	Risk Executive, Security Control Assessor

1.7 Assignment of Security Responsibility

Table 11: [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 12: 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 13: Information System Operational Status

Initiation	Development	Implementation	Operational

1.9 Information system Type

[Enter an "X" in the applicable section] ← DELETE
Table 14: Information System Type

Subsystem/Application	Major Application	General Support System

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 15: 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. *[If the software and/or hardware inventories are large they should be included as appendices to this document, or as standalone documents noted in section 3.1.]*

Table 16: [System Acronym] Hardware Components

Type	Model	Quantity	Manufacturer	Operating System	Location
EXAMPLE: Internet Hosting Server	ML350G2	1	Hewlett Packard	Linux Redhat 4.0 Server	Baltimore, MD Operations Data Center

Table 17: [System Acronym] Software Components

Type	Model	Quantity	Manufacturer	Software	Location
EXAMPLE: Apache Web Server (Cofcws10) Velma	Custom	1	PSC LABS	Linux Redhat 4.0 Server Linux Redhat 4.0 Server Apache Tomcat Version 2.0.52-38	Fort Collins, CO

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 18: [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.

2.1.1 Access 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*]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

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

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

Implementation Statement:
AC-1

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Access Controls**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AC-2]**	
Implementation Statement: **AC-2** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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

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

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

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

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	**Access Control**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AC-3]**	

Implementation Statement:
AC-3

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Access Control**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AC-4]**	

Implementation Statement:
AC-4

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Access Control**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AC-5]**	

Implementation Statement:
AC-5

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Access Controls**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AC-6]**	

Implementation Statement:
AC-6

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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

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

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

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

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	**Access Control**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AC-7]**	

Implementation Statement:
AC-7

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Access Control**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AC-8]**	
Implementation Statement: **AC-8**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Access Control**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AC-11]**	

Implementation Statement: **AC-11** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **Comments:**
Implementation Statement: **AC-11(1)** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Access Control**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AC-12]**	
Implementation Statement: **AC-12** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Access Control**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AC-14]**	
Implementation Statement: **AC-14**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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

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

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

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

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

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	**Access Control**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AC-18]**	
Implementation Statement: **AC-18** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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	Access Control	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	[AC-19]	
Implementation Statement: **AC-19** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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	Access Control	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	[AC-20]	

Implementation Statement:
AC-20

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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

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	**Access Control**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AC-21]**	
Implementation Statement: **AC-21**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Access Control**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AC-22]**	
Implementation Statement: **AC-22**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
Comments:		

2.1.2 Awareness 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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AT-1]**	
Implementation Statement: **AT-1**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Awareness and Training**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AT-2]**	
Implementation Statement: **AT-2** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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	**Awareness and Training**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AT-3]**	
Implementation Statement: **AT-3** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AT-4]**	
Implementation Statement: **AT-4**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
Comments:		

2.1.3 Audit 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	**Audit and Accountability**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AU-1]**	

Implementation Statement:
AU-1

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Audit and Accountability**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AU-2]**	

Implementation Statement:
AU-2

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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
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	**Audit and Accountability**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AU-3]**	
Implementation Statement: **AU-3**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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		
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	**Audit and Accountability**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AU-4]**	
Implementation Statement: **AU-4**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Audit and Accountability**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AU-5]**	
Implementation Statement: **AU-5**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Audit and Accountability**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AU-6]**	
Implementation Statement: **AU-6** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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 **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].

<table>
<tr><td><b>NIST SP 800-53</b></td><td><b>Audit and Accountability</b></td><td rowspan="2">□ Common (Fully Inherited Control)
□ Hybrid (Partially Inherited Control)
□ System Specific Control</td></tr>
<tr><td><b>Revision 4</b></td><td><b>[AU-7]</b></td></tr>
<tr><td colspan="3"><b>Implementation Statement: Does not apply to Low systems according to NIST SP 800-53 Rev 4.</b>
<b>AU-7</b>

<b>Implementation Status:</b> Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

<b>Comments:</b></td></tr>
<tr><td colspan="3"><b>Implementation Statement:</b>
<b>AU-7(1)</b>

<b>Implementation Status:</b> Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

<b>Comments:</b></td></tr>
</table>

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	**Audit and Accountability**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AU-8]**	
Implementation Statement: **AU-8** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AU-9]**	

Implementation Statement: **AU-9**
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable
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
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) □ System Specific Control
Revision 4	**[AU-11]**	
Implementation Statement: **AU-11**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Audit and Accountability**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[AU-12]**	
Implementation Statement: **AU-12** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **Comments:**		

2.1.4 Security 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	**Security Assessment and Authorization**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CA-1]**	

Implementation Statement:
CA-1

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Security Assessment and Authorization**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CA-2]**	

Implementation Statement:
CA-2

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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 **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	**Security Assessment and Authorization**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CA-3]**	
Implementation Statement: **CA-3** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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	**Security Assessment and Authorization**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CA-5]**	
Implementation Statement: **CA-5**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Security Assessment and Authorization**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CA-6]**	
Implementation Statement: **CA-6**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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 freq*uencies] for monitoring and [*Assignment: organization-defined freq*uencies] 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) □ Hybrid (Partially Inherited Control)
Revision 4	**[CA-7]**	□ System Specific Control

Implementation Statement:
CA-7

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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	**Security Assessment and Authorization**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[CA-9]**	□ System Specific Control

Implementation Statement:
CA-9

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

Comments:

2.1.5 Configuration 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	**Configuration Management**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CM-1]**	
Implementation Statement: **CM-1**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CM-2]**	

Implementation Statement:
CM-2

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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

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
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	**Configuration Management**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CM-3]**	
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 **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 **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	**Configuration Management**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[CM-4]**	□ System Specific Control
Implementation Statement: **CM-4** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Configuration Management**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[CM-5]**	□ System Specific Control

Implementation Statement: **CM-5** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Configuration Management**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CM-6]**	
Implementation Statement: **CM-6** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Configuration Management**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CM-7]**	
Implementation Statement: **CM-7** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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		

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 **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 **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	**Configuration Management**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[CM-8]**	□ System Specific Control
Implementation Statement: **CM-8** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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 **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

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	**Configuration Management**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CM-9]**	

Implementation Statement:
CM-9

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Configuration Management**	□ Common (Fully Inherited Control)

Revision 4	**[CM-10]**	□ 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

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	**Configuration Management**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[CM-11]**	□ System Specific Control

Implementation Statement:
CM-11

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

Comments:

2.1.6 Contingency 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	**Contingency Planning**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CP-1]**	

Implementation Statement:
CP-1

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	Contingency Planning	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	[CP-2]	

Implementation Statement:
CP-2

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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

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

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	**Contingency Planning**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CP-3]**	

Implementation Statement:
CP-3

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Contingency Planning**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CP-4]**	
Implementation Statement: **CP-4** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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	**Contingency Planning**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CP-6]**	

Implementation Statement:
CP-6

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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

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	**Contingency Planning**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CP-7]**	

Implementation Statement:
CP-7

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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

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

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	**Contingency Planning**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CP-8]**	

Implementation Statement:
CP-8

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

Comments:

Implementation Statement: **CP-8(1)**
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **Comments:**
Implementation Statement: **CP-8(2)**
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CP-9]**	

Implementation Statement:
CP-9

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[CP-10]**	

Implementation Statement:
CP-10

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

Comments:

Implementation Statement:
CP-10(2)

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

Comments:

2.1.7 Identification 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	**Identification and Authentication**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[IA-1]**	□ System Specific Control

Implementation Statement:
IA-1

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Identification and Authentication**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IA-2]**	

Implementation Statement:
IA-2

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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

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

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

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 **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 **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	**Identification and Authentication**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IA-3]**	
Implementation Statement: **IA-3** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Identification and Authentication**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[IA-4]**	□ System Specific Control
Implementation Statement: **IA-4** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IA-5]**	
Implementation Statement: **IA-5** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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 **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 **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 **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	**Identification and Authentication**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IA-6]**	

Implementation Statement:
IA-6

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Identification and Authentication**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IA-7]**	

Implementation Statement:
IA-7

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Identification and Authentication**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IA-8]**	

Implementation Statement:
IA-8

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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

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

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

Comments:

2.1.8 Incident 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	**Incident Response**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IR-1]**	

Implementation Statement:
IR-1

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Incident Response**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IR-2]**	
Implementation Statement: **IR-2**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Incident Response**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IR-3]**	
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		
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

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	**Incident Response**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IR-4]**	

Implementation Statement:
IR-4

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

Comments:

2.1.8.5 IR-5 Incident Monitoring

The organization tracks and documents information system security incidents.

NIST SP 800-53	**Incident Response**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IR-5]**	
Implementation Statement: **IR-5**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Incident Response**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IR-6]**	
Implementation Statement: **IR-6**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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

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	**Incident Response**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IR-7]**	

Implementation Statement:
IR-7

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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	**Incident Response**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[IR-8]**	
Implementation Statement: **IR-8** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **Comments:**		

2.1.9 Maintenance (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	**Maintenance**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[MA-1]**	
Implementation Statement: **MA-1**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	Maintenance	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	[MA-2]	

Implementation Statement:
MA-2

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	Maintenance	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	[MA-3]	

Implementation Statement:
MA-3

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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	**Maintenance**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[MA-4]**	
Implementation Statement: **MA-4** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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	**Maintenance**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[MA-5]**	
Implementation Statement: **MA-5**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Maintenance**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[MA-6]**	
Implementation Statement: **MA-6**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Media Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[MP-1]**	
Implementation Statement: **MP-1**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Media Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[MP-2]**	
Implementation Statement: **MP-2**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[MP-3]**	
Implementation Statement: **MP-3**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Media Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[MP-4]**	
Implementation Statement: **MP-4**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Media Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[MP-5]**	
Implementation Statement: **MP-5** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[MP-6]**	
Implementation Statement: **MP-6** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Media Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[MP-7]**	
Implementation Statement: **MP-7** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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

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) □ System Specific Control
Revision 4	**[PE-1]**	
Implementation Statement: **PE-1**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Physical and Environmental Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PE-2]**	
Implementation Statement: **PE-2** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Physical and Environmental Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PE-3]**	
Implementation Statement: **PE-3**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Physical and Environmental Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PE-4]**	
Implementation Statement: **PE-4**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Physical and Environmental Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)

Revision 4	[PE-5]	□ System Specific Control
Implementation Statement: **PE-5**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	Physical and Environmental Protection	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	[PE-6]	
Implementation Statement: **PE-6**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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

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	**Physical and Environmental Protection**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Revision 4	**[PE-8]**	

Implementation Statement:
PE-8

Implementation Status: Status (check all that apply):
☐ Implemented (In Place) ☐ Planned (Not in Place) ☐ Compensated ☐ Not Applicable

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	**Physical and Environmental Protection**	☐ Common (Fully Inherited Control) ☐ Hybrid (Partially Inherited Control) ☐ System Specific Control
Revision 4	**[PE-9]**	

Implementation Statement: **PE-9**
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable
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	**Physical and Environmental Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PE-10]**	
Implementation Statement: **PE-10**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Physical and Environmental Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)

Revision 4	**[PE-11]**	□ System Specific Control
Implementation Statement: **PE-11** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Physical and Environmental Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PE-12]**	
Implementation Statement: **PE-12** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Physical and Environmental Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PE-13]**	

Implementation Statement:
PE-13

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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	**Physical and Environmental Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PE-14]**	

Implementation Statement: **PE-14** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Physical and Environmental Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PE-15]**	
Implementation Statement: **PE-15** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 Protection**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PE-16]**	

Implementation Statement: **PE-16**
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable
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) □ System Specific Control
Revision 4	**[PE-17]**	
Implementation Statement: **PE-17**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Planning**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PL-1]**	
Implementation Statement: **PL-1** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**Planning**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PL-2]**	
Implementation Statement: **PL-2** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PL-4]**	
Implementation Statement: **PL-4** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PL-8]**	
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 **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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PS-1]**	
Implementation Statement: **PS-1** **Implementation Status:** Status (check all that apply):		

□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Personnel Security**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PS-2]**	

Implementation Statement:
PS-2

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Personnel Security**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PS-3]**	

Implementation Statement: **PS-3**
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable
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	**Personnel Security**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PS-4]**	
Implementation Statement: **PS-4**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Personnel Security**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PS-5]**	
Implementation Statement: **PS-5**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Personnel Security**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PS-6]**	
Implementation Statement: **PS-6**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Personnel Security**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[PS-7]**	
Implementation Statement: **PS-7**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**Personnel Security**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[PS-8]**	□ System Specific Control

Implementation Statement:
PS-8

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Risk Assessment**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[RA-1]**	□ System Specific Control

Implementation Statement:
RA-1

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[RA-2]**	

Implementation Statement:
RA-2

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**Risk Assessment**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[RA-3]**	

Implementation Statement: **RA-3**
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable
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	**Personnel Security**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[RA-5]**	

Implementation Statement:
RA-5

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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

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

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	**System and Services Acquisition**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SA-1]**	

Implementation Statement:
SA-1

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**System and Services Acquisition**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SA-2]**	

Implementation Statement:
SA-2

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**System and Services Acquisition**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SA-3]**	

Implementation Statement:
SA-3

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**System and Services Acquisition**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SA-4]**	
Implementation Statement: **SA-4**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		

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 **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 **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 **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 **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	**System and Services Acquisition**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[SA-5]**	□ System Specific Control
Implementation Statement: **SA-5**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**System and Services Acquisition**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[SA-8]**	□ 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

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	**System and Services Acquisition**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[SA-9]**	□ System Specific Control

Implementation Statement:
SA-9

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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

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) □ Hybrid (Partially Inherited Control)
Revision 4	**[SA-10]**	□ 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

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	**System and Services Acquisition**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SA-11]**	
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 **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	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-1]**	

Implementation Statement:
SC-1

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-2]**	

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

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	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-3]**	

Implementation Statement:
SC-4

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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) □ Hybrid (Partially Inherited Control)
Revision 4	**[SC-5]**	□ System Specific Control
Implementation Statement: **SC-5**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-7]**	
Implementation Statement: **SC-7**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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

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

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

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

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) □ Hybrid (Partially Inherited Control)
Revision 4	**[SC-8]**	□ System Specific Control
Implementation Statement: **SC-8** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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 **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) □ Hybrid (Partially Inherited Control)
Revision 4	**[SC-10]**	□ System Specific Control
Implementation Statement: **SC-10** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-12]**	
Implementation Statement: **SC-12** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-13]**	
Implementation Statement: **SC-13** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-15]**	
Implementation Statement: **SC-15**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-17]**	
Implementation Statement: **SC-17**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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) □ Hybrid (Partially Inherited Control)
Revision 4	**[SC-18]**	□ System Specific Control

Implementation Statement:
SC-18

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[SC-19]**	□ System Specific Control

Implementation Statement:
SC-19

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-20]**	
Implementation Statement: **SC-20**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-21]**	
Implementation Statement: **SC-21**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-22]**	

Implementation Statement:
SC-22

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

Comments:

2.1.16.17 SC-23 Session Authenticity

The information system protects the authenticity of communications sessions.

NIST SP 800-53	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-23]**	

Implementation Statement:
SC-23

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-28]**	

Implementation Statement:
SC-28

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**System and Communications**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SC-39]**	

Implementation Statement:
SC-39

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**System and Information Integrity**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SI-1]**	
Implementation Statement: **SI-1**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		
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	**System and Information Integrity**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SI-2]**	
Implementation Statement: **SI-2**		
Implementation Status: Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable		

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

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	**System and Information Integrity**	□ Common (Fully Inherited Control)

Revision 4	[SI-3]	□ 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 **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 **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 **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	**System and Information Integrity**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SI-4]**	
Implementation Statement: **SI-4** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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

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

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

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) □ Hybrid (Partially Inherited Control)
Revision 4	**[SI-5]**	□ System Specific Control

Implementation Statement:
SI-5

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SI-7]**	

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

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 **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 **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	**System and Information Integrity**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control) □ System Specific Control
Revision 4	**[SI-8]**	
Implementation Statement: **SI-8** **Implementation Status:** Status (check all that apply): □ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable **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

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

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	**System and Information Integrity**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[SI-10]**	□ 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

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	**System and Information Integrity**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[SI-11]**	□ System Specific Control

Implementation Statement:
SI-11

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**System and Information Integrity**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[SI-12]**	□ System Specific Control

Implementation Statement:
SI-12

Implementation Status: Status (check all that apply):
□ Implemented (In Place) □ Planned (Not in Place) □ Compensated □ Not Applicable

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	**System and Information Integrity**	□ Common (Fully Inherited Control) □ Hybrid (Partially Inherited Control)
Revision 4	**[SI-16]**	□ 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

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
PRIDE	Project Resource Guide
PSC	Program Support Center
RBD	Risk-Based Decision
SAM	Security Authorization Manager
SAR	Security Assessment Report
SBU	Sensitive But Unclassified

TERM	DEFINITION
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.

Term	Definition
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]
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]

Term	Definition
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]
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 Systems and Organizations: Building Effective Assessment Plans, December 2014

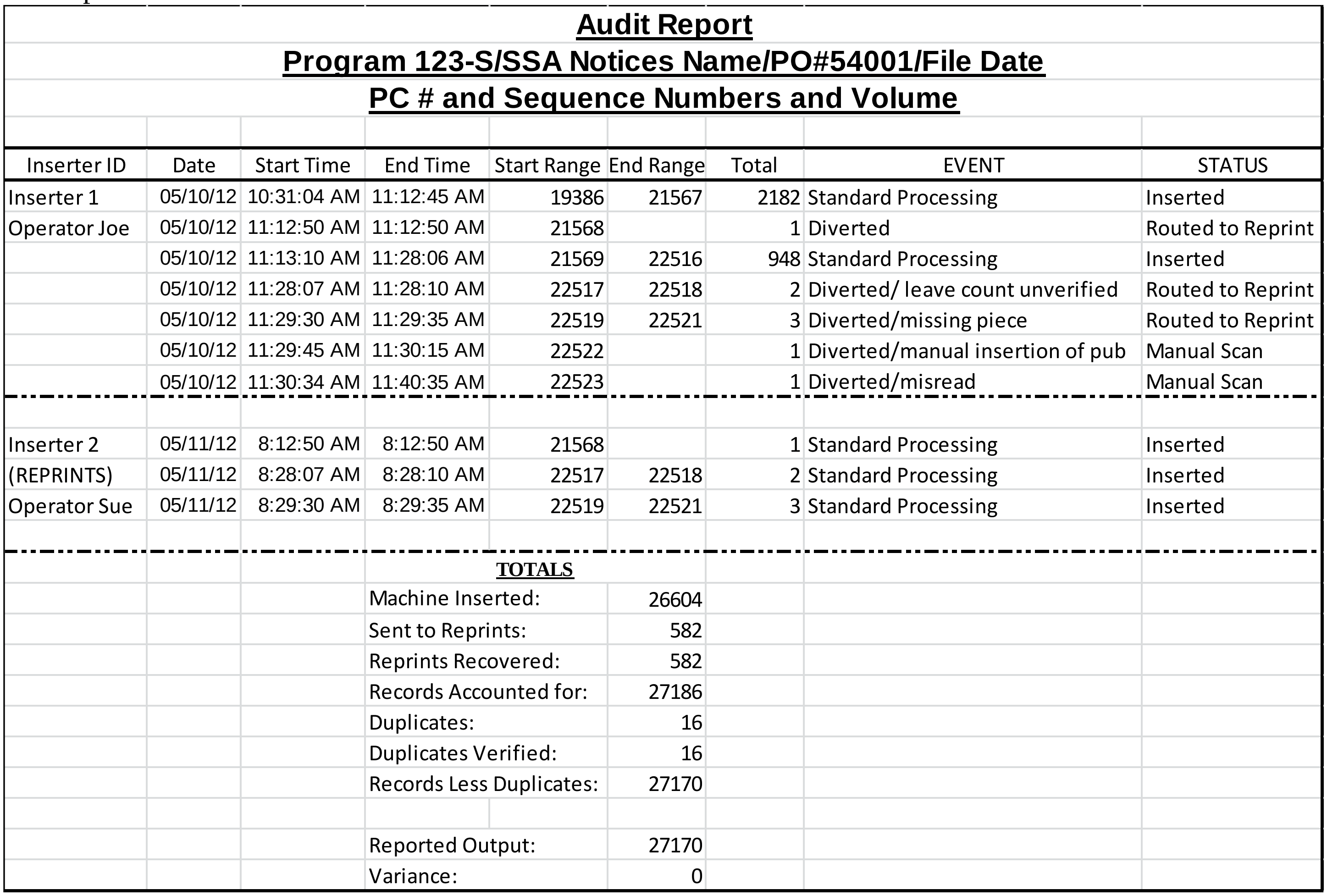
Applicable Laws or Regulations Affecting the System
NIST SP 800-59, Guideline for Identifying an Information System as a National Security System, August 2003.
NIST SP 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.
NIST SP 800-64, 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)

Exhibit H
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:



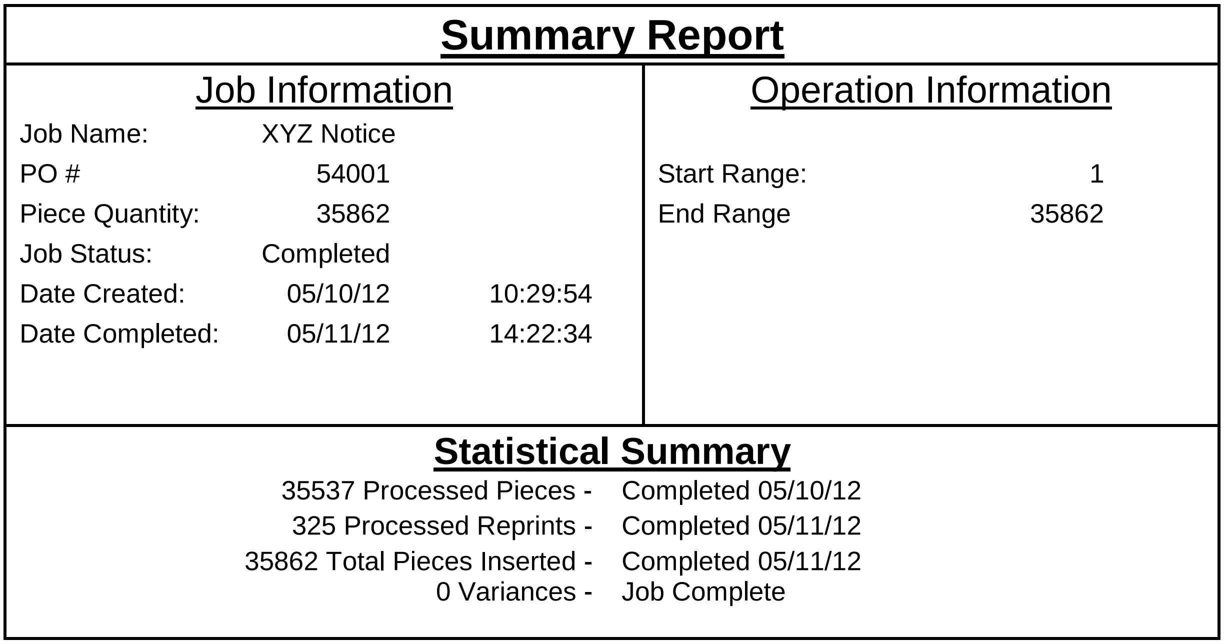
Audit Report
Program 123-S/SSA Notices Name/PO#54001/File Date
PC # and Sequence Numbers and Volume

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 H (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	
Date Created:	05/10/12	10:29:54
Date Completed:	05/11/12	14:22:34

Operation Information

Start Range:	1
End Range	35862

Statistical Summary

35537 Processed Pieces -	Completed 05/10/12
325 Processed Reprints -	Completed 05/11/12
35862 Total Pieces Inserted -	Completed 05/11/12
0 Variances -	Job Complete

EXHIBIT J
Database/Spreadsheet for Postal Documentation

USPS Postage Breakdown

Contractor: ____________________ Date Sent: ____________________

Job Title: ____________________ Mail Date: ____________________ Print Order #: ____________________

Req. #: ____________________ Program #: ____________________ Cost Code: ____________________

Discount	Pieces					Piece Rate					Postage					Total
	1oz	2oz	3oz	4oz	5oz	1oz	2oz	3oz	4oz	5oz	1oz	2oz	3oz	4oz	5oz	
Carrier Route																
5 Digit																
3 Digit																
Automation AADC																
Automation Mixed AADC																
Non Auto. Presort																
Non Auto. Single Piece																
IPA (International Mail)																
Misc. Pieces																
Over 5oz	**No. of Pieces**										**Postage**					

Total USPS Postage	

EXHIBIT J – Mailer 1 – Mid Year Mailer

Enforcement SSA 131 File Layout

Field			***Field***	***SSA***
Location		***Field Name***	***Size***	***131***
01	11	Blank		
12	13	BIC	2	X
14	24	BOAN (999-99-9999)	11	X
25	39	MBR FIRST NAME	15	X
40	40	MBR MIDDLE INITIAL	1	X
41	60	MBR LAST NAME	20	X
61	64	TAX YEAR	4	X
65	70	EARNINGS	6	X
71	79	EIN	9	X
80	119	EMPLOYER ADDRESS – LINE 1	40	X
120	159	EMPLOYER ADDRESS – LINE 2	40	X
160	199	EMPLOYER ADDRESS – LINE 3	40	X
200	239	EMPLOYER ADDRESS – LINE 4	40	X
240	279	EMPLOYER ADDRESS – LINE 5	40	X
280	319	EMPLOYER ADDRESS – LINE 6	40	X
320	333	ZDPC(*ZIP+ZDPC*)	14	X

Exhibit J – Mailer 2 - MYM

ANNUAL EARNINGS TEST MID-YEAR MAILING--VENDOR FILES
(SSA-L9790 - 1 of 2)
(CSMY.WDOC)

Record Location	Field Name	Prog. Pnem.	Field Size	Field Type
1	Data Operation Center		1	A
2	Blank		1	A
3-8	Notice Number		6	AN
9-18	Zip Code + 4		10	NC
19-32	Barcode Print Representation		14	NC
33	PSC		1	N
34	Blank		1	A
35-45	Claim Account Number		11	NC
46	Blank		1	A
47-48	Beneficiary Identification Code (BIC)		2	AN
49	Blank		1	A
50-74	Beneficiary Name		25	ANC
75-96	Beneficiary Address - Line 1		22	ANC
97-118	Beneficiary Address - Line 2		22	ANC
119-140	Beneficiary Address - Line 3		22	ANC
141-162	Beneficiary Address - Line 4		22	ANC
163-184	Beneficiary Address - Line 5		22	ANC
185-203	Blank		19	A
204-206	Group Number		3	AN
207-208	Blank		2	A
209-308	NonWork Months (NWM)		100	ANC

309-310	Blank	2	A
311-315	Month and Year of Full Retirement Age Attainment	5	NC
316-317	Blank	2	A
318-322	Date of Entitlement Current	5	NC
323-324	Blank	2	A
325-328	Tax Year	4	N
329	Blank	1	A
330-335	Annual Exempt Amount ($$,$$$)	6	NC
336	Blank	1	A
337-341	Monthly Exempt Amount ($,$$$)	5	N
342	Blank	1	A
343-362	Spaces	20	ANC

Additional information:

Record Location 209-308 Nonwork Months (NWM)

When the fill-in = NONE (THIS MEANS THAT OUR RECORDS INDICATE YOU ARE WORKING IN EVERY MONTH IN **YYYY),** the year fill-in should be obtained from record location 325-328.

SUMMARY

DATE	**PAGE #**	**EXPLANATION OF CHANGE**
10/22/10		Updated the record location layout with the Special Notice Option (SNO) Code, SNO Priority Code and the

Exhibit J – Mailer 2 - MYM

	Telephone Number for beneficiaries, who are blind or visually imparied.
04/28/11	Updated the requirements with the file names for the vendor, WBDOC and NTIS.
05/04/11	To correct the numbers for he record location.

Exhibit J – Mailer 2 - MYM

ANNUAL EARNINGS TEST MID-YEAR MAILING--VENDOR FILES
(SSA-L9790 – 2 of 2)
(CSMY.WDOC)

Record Location	Field Name	Prog. Pnem.	Field Size	Field Type
1	Data Operation Center		1	A
2	Blank		1	A
3-8	Notice Number		6	AN
9-18	Zip Code + 4		10	NC
19-32	Barcode Print Representation		14	NC
33	PSC		1	N
34	Blank		1	A
35-45	Claim Account Number		11	NC
46	Blank		1	A
47-48	Beneficiary Identification Code (BIC)		2	AN
49	Blank		1	A
50-74	Beneficiary Name		25	ANC
75-96	Beneficiary Address - Line 1		22	ANC
97-118	Beneficiary Address - Line 2		22	ANC
119-140	Beneficiary Address - Line 3		22	ANC
141-162	Beneficiary Address - Line 4		22	ANC
163-184	Beneficiary Address - Line 5		22	ANC
185-203	Blank		19	A
204-206	Group Number		3	AN
207-208	Blank		2	A
209-308	NonWork Months (NWM)		100	ANC
309-310	Blank		2	A
311-315	Month and Year of Full Retirement Age Attainment		5	NC

Exhibit J – Mailer 2 - MYM

316-317	Blank	2	A
318-322	Date of Entitlement Current	5	NC
323-324	Blank	2	A
325-328	Tax Year	4	N
329	Blank	1	A
330-335	Annual Exempt Amount ($$,$$$)	6	NC
336	Blank	1	A
337-341	Monthly Exempt Amount ($,$$$)	5	N
342	Blank	1	A
343	Special Notice Option (SNO) Code	1	N
344-346	Telephone Area Code	3	N
347	Dash	1	C
348-350	Telephone Exchange	3	N
351	Dash	1	C
352-355	Telephone Number	4	N
356	Dash	1	C
357-361	Telephone Extension	5	N
362	Special Notice Option Priority Code	1	A

Additional information:

Record Location 209-308 Nonwork Months (NWM)

When the fill-in = NONE (THIS MEANS THAT OUR RECORDS INDICATE YOU ARE WORKING IN EVERY MONTH IN YYYY), the year fill-in should be obtained from record location 325-328.

Exhibit J – Mailer 2 - MYM

The Special Notice Option Priority Code isn't on the SNO database. It's a field that NTIS requested us to send them with an 'S' in it, record location is 362. The SNO Priority Code is only for SNO values equal to 3, 4, 6 or 7.

NOTE:

A file for the data derived from record location 343 (SNO CODE) should be sent out accordingly:

SNO CODE 3, 4, 6 and 7 goes to NTIS and to the print vendor.

SNO CODE 2 goes to WBDOC and to the print vendor. This is the only option that should have a telephone number associated with it.

SUMMARY

DATE	PAGE #	EXPLANATION OF CHANGE
10/22/10		Updated the record location layout with the Special Notice

Exhibit J – Mailer 2 - MYM

	Option (SNO) Code, SNO Priority Code and the Telephone Number for beneficiaries, who are blind or visually imparied.
04/28/11	Updated the requirements with the file names for the vendor, WBDOC and NTIS. To add Attachment 2 for when SNO values equal 2, 3, 4, 6 or 7.
05/04/11	To correct the numbers for the record location.

Exhibit J – Mailer 3 & 4 – MYM

ANNUAL EARNINGS TEST MID-YEAR MAILING--VENDOR TAPE FILES (CSMY.WDOC)

Record Location	Field Name	Prog. Pnem.	Field Size	Field Type
1	Data Operation Center = W		1	A
2-7	Notice code - 9781, 9778S, 9779S, 9784SM, 9785SM		6	AN
8-12	Zip		5	N
13	Dash		1	C
14-17	Zip+4		4	N
18-31	Barcode Print Representation		14	NC
32	PSC		1	N
33-35	Claim Account Number Area		3	N
36	Dash		1	C
37-38	Claim Account Number Group		2	N
39	Dash		1	C
40-43	Claim Account Number Serial		4	N
44-45	Beneficiary Identification Code (BIC)		2	AN
46-55	Beneficiary Given Name (BGN)		10	ANC
56	Beneficiary Middle Initial (BMI)		1	ANC
57-68	Beneficiary Last Name (BGN)		12	ANC
69-90	Beneficiary Address 1		22	ANC
91-112	Beneficiary Address 2		22	ANC
113-134	Beneficiary Address 3		22	ANC
135-156	Beneficiary Address 4		22	ANC

Exhibit J – Mailer 3 & 4 – MYM

157-178	Beneficiary Address 5	22	ANC
179-187	Amount of Reported Earnings(AORE)	9	NC
188-197	First Nonwork Month	10	A
198-200	Group Number	3	AN
201-300	NonWork Months (NWM)	100	ANC
301-302	Date of Entitlement Current (DOEC) MM	2	NC
303	Slash	1	C
304-305	Date of Entitlement Current (DOEC) YY	2	NC
306-310	Month and Year of Full Retirement Age Attainment MM/YY	5	NC
311-320	Month (spelled out) of FRA attainment.	10	C
321-322	Year of FRA CC	2	NC
323-324	Year of FRA YY	2	NC
325-325	Special Notice Option (SNO) Code	1	N
326-328	Telephone Area Code	3	N
329	Dash	1	C
330-332	Telephone Exchange	3	N
333	Dash	1	C
334-337	Telephone Number	4	N
338	Special Notice Option Priority Code	1	A
339-350	Space	12	

Additional information:

SSA-L9784 and SSA-L9785 (only). The fill-in for “f” should be shown (spelled out) as month. The field size should be 10 characters to accommodate the longest month. The data for this fill-in will be obtained from record location 311-320.

SSA – L9778, SSA-L9779 and SSA-L9781 coversheet page 2 fill-in the month in the fill-in for “a” should be shown (spelled out) as month. The field size should be 10 characters to accommodate the longest month. The data for this fill-in will be obtained from record location 311-320. The year fill-in for “b” should be obtained from record location 321-324.

NOTE:

A file for the data derived from record location 325 (SNO CODE) should be sent out accordingly:

SNO CODE 3, 4, 6 and 7 goes to NTIS and to the print vendor.
SNO CODE 2 goes to WBDOC and to the print vendor.
SNO CODE 1 goes to the print vendor.

Exhibit J – Mailer 3 & 4 – MYM

SUMMARY

DATE	PAGE #	EXPLANATION OF CHANGE
10/22/10		Updated the record location layout with the Special Notice Option (SNO) Code and the Telephone Number for beneficiaries, applicants, recipients and representative payees who are blind or visually imparied.
02/24/11		Added verbage for who to send a file to for the various SNO CODEs.

Exhibit J – Mailer 3 & 4 – MYM

Request for Operational Support
Current Year (CCYY) Annual Earnings Test Mid-Year Mailing (MYM) Operation
TABLE LOG FOR YEARLY UPDATES

Effective Date	**AORE**	**Current Year (CCYY)**	**Prospective Year (CCYY)**	**Prior Year (CCYY)**	**Special Updates**
04/2009	$14,161 (under FRA) $37,682 (FRA and over)	2009	2010	2008	Due to the Version 15 MBR rewrite, the Disability BIT code is now obsolete. References to the BIT code have been replaced by BCLM CEC • B.
04/2010	$14,161 (under FRA) $37,682 (FRA and over)	2010	2011	2009	None
04/2011	$14,161 (under FRA) $37,682 (FRA and over)	2011	2012	2010	Updated the functional requirement to call the SNO database to obtain the SNO code and telephone number for beneficiaries, applicants, recipients and representative payees who blind or visually impaired.

A. Background

Exhibit J – Mailer 3 & 4 – MYM

The MYM operation is the vehicle to identify beneficiaries who are likely not to report an earnings estimate or underestimate their earnings. The MYM operations’ goal is to obtain as many current year estimates and future estimates as possible. This is to allow as many beneficiaries to report for the future year due to the elimination of the Annual Report Process effective January 1997. An initial roundup selection is made in July for all risk groups identified below, and a continuing monthly selection for beneficiaries in the retirement risk group in August through October.

This request provides the criteria for selecting these beneficiaries and extracting the necessary MBR Data for completing the earnings estimate notice.

B. Processing

1. Initial Roundup Selection (July)

a. Search and select from the MBR file all records, which meet the criteria outlined in Selection Criteria 1 below. This operation must search each MBR for all selection criteria. The selected records in this search are to be maintained in an SC1 file, as a further sort is required (B.l.b below).

NOTE: If a selected record in any group does not have a zip code, then drop the record.

Selection Criteria 1 (SCl File)

a) BIC = A, B (any subscript), D (any subscript) or E (any subscript)
b) LAF = C or D or S2 with a WKCON WCD field present < 01/**Prospective Year (Current Year + 1)**
c) FRA > **Current Year (CCYY)**
d) DOEC < 01/**Prospective Year (Current Year + 1)**
e) BIC is not entitled to DIB, (i.e. BCLM-CEC ≠ B
f) PC ≠ 8

b. The above SC1 file, in B.l.a., will be further sorted into the following selection groups. One item (one identified BIC) only can be selected in one group's criteria that it meets. Once the item has been identified for a group, it should be tagged as such and eliminated from further screening.

l) Group sort criteria for SCl

SCREENING AND SELECTION PRIORITY:
Group 7A and 7B selection criteria has priority over all other groups within the SCl file, and therefore has been listed in selection priority.

Groups 16A, 16B, 17 and 18 selection criteria has priority over Groups 4, 6 and 9 selection criteria respectively,and therefore has been listed in selection priority. Thus,Group 3 has selection priority over all other remaining Groups (4-6, 8, 9, 14 through 20), and so forth.

All selected records will be reflected on the CSMY.WDOC file.

a) Group 7A

* (1) DOEC = 02/**Current Year (CCYY)** through 07/**Current Year (CCYY)**

* (2) ARD occurrence with YOER = **Current Year (CCYY)** is present, <u>and</u>

Note! The MBR can now reflect 2 ARD occurrences for the same year. Therefore, if the TOW = F in one of the occurrences, do not select the record. This note applies throughout the spec wherever we look at ARD.

* (a) **Current Year (CCYY)** AORE > **AORE**

* (3) Every month in the ARD-NON-WK-MTH field contains a "Y" from the DOEC through 12/**Current Year (CCYY)**.

Example: The beneficiary's DOE is 06/**Current Year (CCYY)**. The ARD-NON-WK-MTH field contains a "Y" in the 1st and 6th through 12th positions indicating NWM's of 01/**Current Year (CCYY)** and 06/**Current Year (CCYY)**-12/**Current Year (CCYY)**. Select the record.

b) Group 7B

* (1) DOEC = 02/**Current Year (CCYY)** through 07/**Current Year (CCYY)**

* (2) ARD occurrence with YOERs = **Prior Year (CCYY**) and **Current Year (CCYY)**are present, <u>and</u>

Exhibit J – Mailer 3 & 4 – MYM

* (a) **Current Year (CCYY) AORE** < **AORE and Prior Year (CCYY) AORE > AORE**

* (3) Every month in the ARD-NON-WK-MTH field contains a "Y" from the DOEC through 12/**Current Year (CCYY)**.

Example: The beneficiary's DOE is 06/**Current Year (CCYY)**. The ARD-NON-WK-MTH field contains a "Y" in the 1st and 6th through 12th positions indicating NWM's of 01/**Current Year (CCYY)** and 06/**Current Year (CCYY) through** 12/**Current Year (CCYY)**. Select the record.

c) Group 3

* (1) ARD occurrences with YOER's = **Prior Year (CCYY)** and **Current Year (CCYY)** are present, <u>and</u>

* The AORE for **Current Year (CCYY)** > **AORE** <u>and</u> the AORE for **Prior Year (CCYY)** > AORE for **Current Year (CCYY)**

* (2) BCLM-LMETY ≠ **Current Year (CCYY)** or blank

d) Group 16A

* (1) DOEC ≠ 08/**Current Year (CCYY)**, 09/**Current Year (CCYY)** or 10/**Current Year (CCYY)**

* (2) The 12th position of the ARD-NON-WK-MTH = Y in the YOER = **Current Year (CCYY)**(therefore December is a non-service month) <u>and</u>

* (3) ARD occurrences with YOER's = **Prior Year (CCYY)** and **Current Year (CCYY)** are present, <u>and</u>

The AORE for **Current Year (CCYY)** > **AORE** <u>and</u> the AORE for **Prior Year (CCYY)** > AORE for **Current Year (CCYY)**

* (4) If the DOEC ≥ 01/**Current Year (CCYY)**; at least one month from the DOEC through **12/Current Year (CCYY)** period contains a <u>work</u> month reflected in the **Current Year (CCYY)** ARD-NON-WK-MTH field. At least one of the 12 positions contains an "N"

* (5) BCLM-LMETY = **Current Year (CCYY)** or blank

e) Group 16B

Exhibit J – Mailer 3 & 4 – MYM

*   (1) DOEC ≠ 08/**Current Year (CCYY)**, 09/**Current Year (CCYY)** or 10/**Current Year (CCYY)**

*   (2) The 12th position of the ARD-NON-WK-MTH = Y in the YOER = **Current Year (CCYY)(**therefore December is a non-service month)   and

*   (3) ARD occurrences with YOER's = **Prior Year (CCYY)** and **Current Year (CCYY)** are present,   and

The AORE for **Current Year (CCYY)** < **AORE** and the AORE for **Prior Year (CCYY)** > **AORE**

(4) If the DOEC ≥ 01/**Current Year (CCYY)**; at least one month from the DOEC through **12/Current Year (CCYY)** period contains a work month reflected in the **Current Year (CCYY)** ARD-NON-WK-MTH field. At least one of the 12 positions contains an "N"

*   (5) BCLM-LMETY = **Current Year (CCYY)** or blank

f)   Group 4

*   (1) ARD occurrences with YOER's = **Prior Year (CCYY)** and **Current Year (CCYY)** are present,   and
*
The AORE for **Current Year (CCYY)** > **AORE** and the AORE for **Prior Year (CCYY)** > AORE for **Current Year (CCYY)**

*   (2) If the DOEC ≥ 01/**Current Year (CCYY)**; at least one month from the DOEC through **12/Current Year (CCYY)** period contains a work month reflected in the **Current Year (CCYY)** ARD-NON-WK-MTH field. This means at least one of the 12 positions must contain an "N" or the NONWORK MONTHS field is not present beginning with the DOEC.

*   (3) BCLM-LMETY = **Current Year (CCYY)** or blank

g)   Group 5

*   (1) ARD occurrences with YOER's = **Prior Year (CCYY)** and **Current Year (CCYY)** are present,   and

The AORE for **Current Year (CCYY)** > **AORE** and the AORE for **Current Year (CCYY)** ≥ AORE for **Prior Year (CCYY)**

*   (2) BCLM-LMETY ≠ **Current Year (CCYY)** or blank

h)   Group 17

*   (1) DOEC ≠ 08/**Current Year (CCYY)**, 09/**Current Year (CCYY)** or 10/**Current Year (CCYY)**

*   (2) The 12th position of the ARD-NON-WK-MTH field contains a "Y" in the YOER = **Current Year (CCYY)** and

*   (3) ARD occurrences with YOER's = **Prior Year(CCYY)** and **Current Year (CCYY)** are present,   and

The AORE for **Current Year (CCYY)** > **AORE** but the AORE for **Current Year (CCYY)** ≥ AORE for **Prior Year (CCYY)**

*   (4) If the DOEC ≥ 01/**Current Year (CCYY)**; at least one month from the DOEC through 12/**Current Year (CCYY)** period contains a work month reflected in the **Current Year(CCYY)** ARD-NON-WK-MTH field. At least one of the 12 positions must contain an "N"

*   (5) BCLM-LMETY = **Current Year (CCYY)** or blank

i)   Group 6

*   (1) ARD occurrences with YOER's = **Prior Year(CCYY)** and **Current Year (CCYY)** are present,   and

The AORE for **Current Year (CCYY)** > **AORE** but the AORE for **Current Year (CCYY)** ≥ AORE for **Prior Year (CCYY).**

*   (2) If the DOEC ≥ 01/**Current Year (CCYY)**; at least one month from the DOEC through 12/**Current Year (CCYY)** period contains a work month reflected in the **Current Year (CCYY)** ARD-NON-WK-MTH field. This means at least one of the 12 positions must contain an "N" or the NONWORK MONTHS field is not present beginning with the DOEC.

*   (3) BCLM-LMETY = **Current Year (CCYY)** or blank

j)   Group 8

*   (1) ARD occurrence with a YOER = **Current Year(CCYY)** is present, but a YOER = **Prior Year(CCYY)** is not present,   and

*   AORE for **Current Year (CCYY)** > **AORE**

Exhibit J – Mailer 3 & 4 – MYM

* 2) BCLM-LMETY ≠ **Current Year (CCYY)** or blank

k) Group 18

* (1) DOEC ≠ 08/**Current Year (CCYY)**, 09/**Current Year (CCYY)** or 10/**Current Year (CCYY)**

* (2) The 12th position of the ARD-NON-WK-MTH field contains a "Y" in the YOER = **Current Year (CCYY)** and

* (3) ARD occurrence with a YOER = **Current Year (CCYY)** is present, but a YOER = **Prior Year(CCYY)** is not present, and

* AORE for **Current Year (CCYY)** > **AORE**

* (4) If the DOEC ≥ 01/**Current Year (CCYY)**; at least one month from the DOEC through 12/**Current Year (CCYY)** period contains a work month reflected in the **Current Year(CCYY)** ARD-NON-WK-MTH field. At least one of the 12 positions must contain an "N"

* (5) BCLM-LMETY = **Current Year (CCYY)** or blank

l) Group 9

* (1) ARD occurrence with a YOER = **Current Year(CCYY)** is present, but a YOER = **Prior Year (CCYY)** is not present, and

* AORE for **Current Year (CCYY)** > **AORE**

* (2) If the DOEC ≥ 01/**Current Year (CCYY)**; at least one month from the DOEC through 12/**Current Year (CCYY)** period contains a work month reflected in the **Current Year (CCYY)** ARD-NON-WK-MTH field. At least one of the 12 positions must contain an "N" or the NONWORK MONTHS field is not present beginning with the DOEC.

* (3) BCLM-LMETY = **Current Year (CCYY)** or blank

GROUPS 14 AND 15 SELECTIONS ARE FOR STUDY PURPOSES ONLY.
DO NOT BUILD A RECORD ON THE CSMY.WDOC FILE.

m) Group 14

* (1) ARD occurrences with a YOER = **Prior Year (CCYY)** is present, but a YOER = **Current Year (CCYY)** is not present, <u>and</u>

* AORE for **Prior Year (CCYY)** > **AORE**

* (2) The 12th position of the ARD-NON-WK-MTH field contains a "Y" in the YOER = **Current Year (CCYY)** <u>and</u>

* (3) WIC = 2 is present for at least one month in **Current Year (CCYY)**, <u>and</u>

* (4) BCLM-LMETY ≠ **Current Year (CCYY)** or blank

n) Group 15

* (1) ARD occurrences with a YOER = **Prior Year (CCYY)** is present, but a YOER = **Current Year (CCYY)** is not present, <u>and</u>

* AORE for **Prior Year (CCYY)** > **AORE**

* (2) The 12th position of the ARD-NON-WK-MTH field contains a "Y" in the YOER = **Current Year (CCYY)** <u>and</u>

* (3) WIC = 2 for at least one month in **Current Year (CCYY)**, <u>and</u>

* (4) BCLM-LMETY = **Current Year (CCYY)** or blank

2) Work Notice Fallout Record File

* Any record not meeting SC1 <u>or</u> groups 3 through 9, 14 through 20 criteria should be stored in a work notice fallout file. An MBR LIMIT listing of these records should be produced during the roundup and monthly validation tasks of this selection operation.

3) WRK AJS Files

* Process MIA transactions created by the July RETAP selection through AJS-3. The TID:MIA transactions will post a WKCON MYMI = **11** on the MBR for Groups 3 through 6, 8 and 9. The MIA transactions will be on the following file: CSAJSII7

Exhibit J – Mailer 3 & 4 – MYM

MIA transactions are to be built as follows:

CAN999999999A.TIDMIA.CLNXXXXX,XXX.YOR**11**.
DON0718**11**.AIDMYMIANNO.PSC9.

Cross refer to Non Responder Specifications SR# 35517 and 35517A, B and C, Function 1.1, 1.2 & 2.0.

3. Group 19 and 20

Selection of beneficiary attaining FRA
SC 3 Initial Roundup Selection FRA in **Current Year (CCYY)** February **Current Year (CCYY)**-December **Current Year (CCYY)**

Initial Roundup Selection (July)

Search and select from the MBR file all records that meet the criteria outlined in Selection Criteria 3 below. This operation must search each MBR for all selection criteria. The records selected in this search must be maintained in an SC3 files as a further sort is required (See below).

NOTE: If a selected record in any group does not have a zip code, the record is dropped.

Selection Criteria 3 (SC3 File)

a) BIC = A,B (any subscript), D (any subscript) or E (any subscript)
b) The LAF is equal to C, D or S2
c) The AORE for **Current Year (CCYY)** is > **37682** or there is a WIC of 2 in any month in year **Current Year (CCYY)**
d) FRA > 01/**Current Year (CCYY)** and < 01/**Prospective Year (Current Year + 1)** (attainments February - December)
e) DOEC < FRA
f) BIC is <u>not</u> entitled to DIB, that is BCLM-CEC ≠ B
g) PC ≠ 8

The above SC3 file, will be further sorted into the following selection groups. Once the item has been identified for a group, it should be tagged as such and eliminated from further screening.

Group 19 – BCLM-LMETY ≠ **Current Year (CCYY)** or blank
(LMETY has been used)
Group 20 – BCLM-LMETY = **Current Year (CCYY)** or blank
(LMETY has not been used)

2. Continuing Month Selection (August through October)

a. This selection will be made monthly, beginning with August and ending with October. Each month, select all beneficiaries whose record contains the following:

Identify all items in this selection as Group 7A Monthly. All records selected are reflected on the CSMY.WDOC file.

1) BIC = A, B (any subscript), D (any subscript) or E (any subscript)

2) LAF = C or D

* 3) FRA > **Current Year (CCYY)**

4) DOEC = the current selection month and the year is **Current Year (CCYY)** (i.e., first selection month is August, therefore DOEC = 08/**Current Year (CCYY)**.)

5) ARD is present, <u>and</u>

* a) YOER = **Current Year (CCYY)** and the TOER = "W"

b) AORE is present, and

* AORE > **AORE**

* c) Every month in the DOEC through 12/**Current Year (CCYY)** period is reflected as a non-work month in the ARD-NON-WK-MTH field.

6) BIC's BCLM-CEC ≠ B

7) PC ≠ 8

b. This selection will be made monthly, beginning with August and ending with October. Each month, select all beneficiaries whose record contains the following:

Identify all items in this selection as Group 7B Monthly. All records selected will be reflected on the CSMY.WDOC file.

1) BIC = A, B (any subscript), D (any subscript) or E (any subscript)

2) LAF = C or D

***** 3) FRA > **Current Year (CCYY)**

4) DOEC = the current selection month and the year is **Current Year (CCYY)** (i.e., first selection month is August, therefore DOEC = 08/**Current Year (CCYY)**.)

5) ARD is present, <u>and</u>

***** a) YOER = **Prior Year (CCYY)** and

b) AORE is present and AORE > **AORE**

c) YOER = **Current Year (CCYY)** and the TOER = "W"

b) AORE is present, and AORE < **AORE**

***** c) Every month in the DOEC through 12/**Current Year (CCYY)** period is reflected as a non-work month in the ARD-NON-WK-MTH field.

6) BIC's BCLM-CEC ≠ B

7) PC ≠ 8

4. Each of the groups identified in the initial roundup and monthly selection above will be sent a specific earnings estimate request notice. These notices require various fill-ins.

The notice to be sent to each group and the data required to complete the fillins in these notices, which will either be extracted from the MBR or determined based on the beneficiary's year of birth, are as follows:

(The format for these entries is contained on the Record Specification, Attachment 1.)

a. Notices

If Group is:	Then the notice number is:
3, 5 or 8	SSA-L9778 SUP
4, 6 or 9	SSA-L9779 SUP
7A, 7B 7A monthly, 7B monthly	
16A, 16B, 17 or 18	SSA-L9781 EP
19	SSA-L9784 SM
20	SSA-L9785 SM

b. Data that is to be extracted from the MBR.

1) Program service Center (PSC)

The PSC must be extracted from the Fixed Payment Data and displayed in a one position format.

2) ZIP Code + 4 Extension

The ZIP Code + 4 Extension must also be extracted from the MBR. It should be displayed in 99999-9999 format. If the + 4 extension is blank, missing or invalid, then it should <u>not</u> be displayed within the record, i.e., MBR shows 21061-ƀƀƀƀ, only display 21061.

3) Advanced POSTNET Barcode Print Representation

The POSTNET Barcode will be created and printed directly under the last line of the PNA data <u>only</u> when the 9 digit-ZIP (ZIP + 4) <u>and</u> the zip delivery point code (ZDPC) are present. The Advanced POSTNET Barcode will begin in print position 11 (1 inch from the left edge of the page). The Barcode should use the proportional barcode font MB041P. When the ZDPC is present the barcode print line will reflect the following: *123456789012* which represents the ZIP, ZIP-ADD-ON, AND ZDPC fields on the MBR. The ZDPC consists of 3 digits and will be extracted from the Payment portion of the MBR. If the ZDPC is blank, the POSTNET Barcode should not be generated. If the ZDPC is blank, but the zip and plus 4 extension is present, display the zip and plus 4 extension. See Attachment 7 for additional information on the POSTNET Barcode.

4) Claim Account Number (CAN)

Display the CAN in 999-99-9999 format.

5) Beneficiary's Identification Code (BIC)

The selected beneficiary's BIC will be extracted from the Fixed Beneficiary Data field.

6) Beneficiary's Name

The selected beneficiary's name is <u>always</u> to be extracted from the Fixed Benefit Data portion (BGN, BMI and BLN) of the MBR. The benefit name will be edited to ensure one space before and after the middle initial.

7) Beneficiary's Address

The selected beneficiary's address will be taken from the Payee Name and Address data. The first line of address (FLOA) code will be utilized to determine the start of the beneficiary's address.

8) Amount of Reported Earnings (AORE)

***** Extract the actual **Current Year (CCYY)** AORE from the ARD on the MBR. Display the AORE in $,$$$,$$$ format.

Processing Notes:

a) The AORE must be displayed with a comma when the dollar amount exceeds the hundreds position.

b) If the AORE is less than nine dollar positions, fill the left side positions with <u>blanks</u>.

9) Non-Work Months - (Variable Fillin)

The Non-Work Months, when present for YOER = **Current Year (CCYY)**, will be extracted from the ARD-NON-WK-MTH field of the MBR. For example, if ARD-NON-WK-MTH contains a "Y" in all of the 12 positions the Non- Work Months should be displayed as follows:

JANUARY FEBRUARY MARCH APRIL MAY JUNE JULY AUGUST
SEPTEMBER OCTOBER NOVEMBER DECEMBER

The Non-Work Months must be displayed in calendar sequence (i.e., January prior to February, etc.), including 2 separator spaces after each NWM.

***** If the DOEC $\geq$ 01/**Current Year (CCYY)**, and the DOEI = the DOEC, only Non-Work Months beginning with the DOEC through 12/**Current Year (CCYY)** should be displayed.

If NonWork Months are not present for **Current Year**

(CCYY), The 12 positions in the ARD-NON-WK-MTH field are all blank display:

"None (This means that our records indicate you are working in every month in **Current Year (CCYY)**)".

* 10) Month and Year of FRA Attainment

Extract the date of birth from the Fixed Beneficiary Data field of the MBR. Compute the month and year of FRA attainment using the beneficiary's date of birth. Display in MM/YY format

* 11) Date of Entitlement Current (DOEC)

Extract the beneficiary's DOEC from the Fixed Beneficiary Data field of the MBR. Display in MM/YY format after the month/year of FRA attainment

12) Month of FRA

The month of FRA attainment should be spelled out as month(computed in item 10) only month shown.

13) Month (spelled out) and year of FRA attainment

The month of FRA attainment should be spelled out as month(computed in item 10), only month shown.

Remaining Data Determinations

1) Data Operation center (DOC)

Regardless of the PSC of record, the DOC designator will always be W for Wilkes-Barre DOC.

2) Group Selection Number

Display the group number's criteria that the beneficiary was selected under, i.e., 3 through 7A, 7B, 8, 9 or 16A, 16B through 20.

3) Notice Number

Display the notice number the beneficiary will receive.

If the notice is:	Then Display:
SSA-L9778 SUP	9778S
SSA-L9779 SUP	9779S

SSA-L9781 SM	9781
SSA-L9784 SM	9784
SSA-L9785 SM	9785

14) Call the Special Notice Option (SNO) database to obtain SNO data associated on either a COSSN/CID or CAN/BIC.

REPD-IND = ‘Y’ and RPNI = ‘1’ and TOP • ‘A’ and

- RPN is present, call the SNO database using the RPN to obtain the SPECIAL NOTICE OPTION CODE and the TELEPHONE NUMBER.
    - SPECIAL NOTICE OPTION PRIORITY CODE = ‘S’
- RPN not present do not call the SNO database (a regular notice is sent).

REPD-IND = ‘Y’ and RPNI • ‘1’

- Do not call the SNO database (send out regular notice).

REPD-IND • ‘Y’ <u>or</u> REPD-IND = ‘Y’ and TOP = ‘A’

- Call the SNO database using the COSSN/CID or CAN/BIC to obtain the SPECIAL NOTICE OPTION CODE and the TELEPHONE NUMBER.
    - SPECIAL NOTICE OPTION PRIORITY CODE = ‘S’

15. The fill-ins for the Spanish language notices will be as follows:

The 100 character Spanish legend for the English phrase “NONE, etc” is:

NINGUNO (ESO INDICARÍA QUE NUESTROS REGISTROS MUESTRAN QUE ESTÁ TRABAJANDO TODOS LOS MESES DEL Current Year (CCYY))

The list of months in Spanish corresponding to JANUARY, FEBRUARY, etc is:

ENERO, FEBRERO, MARZO, ABRIL, MAYO, JUNIO, JULIO, AGOSTO, SEPTIEMBRE, OCTUBRE, NOVIEMBRE, DICIEMBRE

The FRA month (maximum of 10 characters) is:

ENERO, FEBRERO, MARZO, ABRIL, MAYO, JUNIO, JULIO, AGOSTO, SEPTIEMBRE , OCTUBRE, NOVIEMBRE, DICIEMBRE

C. Inputs and Outputs

1. Initial Roundup Operation

The output files below, and their user component, for the initial roundup are defined as follows:

a. Vendor File (CSMY.WDOC) - Deliver to vendor

Two files will be created for the vendor. The file names will be OLBG.BTI.CSMY.WDOC. and OLBG.BTI.CSMY.WDOC.S These files will contain notice numbers SSA-L9778 SUP, SSA-L9779 SUP, SSA-L9781 SM, SSA-L9784 SM and SSA-L9785 SM. The file OLBG.BTI.CSMY.WDOC.S will contain any record that has a language code (LANG) of S in BENEFIT data on the MBR. Beneficiaries on this record will receive the Spanish version of the notices listed above. All other processing remains the same. The selection criteria are the same as spelled out in this spec for all selection categories. The only difference is if the LANG equals S they go into this file so they receive a Spanish language notice. The Record Specification for this file is contained on Attachment 1. (NOTE: The 6 position notice number is being retained for other possible test cases in the future). The File Characteristics for these files are contained on Attachment 2.

The above files (CSMY.WDOC) will be released to a contracted vendor for printing of the notices.

b. DOC/Non-Responder Control Files - Deliver to WBDOC

One NDM file will also be created to control the future year estimate responses to all the MYM notices. The file name will be OLBG.BTI.WB2.CSMYWDOB.RYYMMDD. The CSMYWDOB file must contain all 9778-SUP, 9779-SUP, 9781SM, 9784SM and 9785SM records from the WDOC file. One copy of the CSMY.WDOB file should be shipped to WDOC after the initial roundup and each monthly i.e., August, September and October. The format for these files is contained on the Record Specification, Attachment 3. The File Characteristics are contained on Attachment 4. The file must be in
CAN order.

Control Files Data Content

a) CAN

Display the CAN in 999999999 format.

b) BIC

c) Date of Birth (DOB) **(CSMYWDOB FILE)**

Display the DOB in MM/DD/YY format, obtained from the Benefit Data portion of the MBR.

NOTE: This file now will be created under the National Data Mover (NDM) facility.

c. ZIP Code Listing **(CSWDOCZP.R02MMDD FILE)** - **Deliver to ORSIS**

This listing will display a count, in ZIP CODE sequence, only using 5 digit zip, of the records selected for each ZIP CODE. One listing will be produced for the CSMY. WDOC tape file. A facsimile of the ZIP CODE listing is contained on Attachment 5.

d. Test Record Listing and MBR Printouts - **Deliver to ORSIS**

These listings and materials will be used to assess the quality of the vendor product and the selection operation.

Produce two print listings, one for the vendor and one for Printing Management Team for the CSMY.WDOC tape file as follows:

CSMY.WDOC (MYM1 FILE)

Display the first 100 items selected for <u>each</u> notice SSA-L9778 SUP, SSA-L9779 SUP SSA-L9781 SM, SSA-L9784 SM and SSA-L9785 SM) within WDOC file.

(Total selection 500 items per file).

All records selected will be on the CSMY.WDOC file.

e. Mid-Year Mailing Statistics and MBR Limit Printouts - **Deliver to ORSIS for OQP**

1) A totals report will be created for the Wilkes-Barre Data Operation Center.

The report will include:

a) A breakout of the selection groups (3 through 7, 8, 9, 16 through 20) and the number of each BIC = A, B, D or E selected within those groups.

b) The number of beneficiaries meeting the selection universe of SCl and SC3.

c) The number of input beneficiaries who were not selected in any of the 14 groups. Thus, the beneficiary met the criteria for selection in SC1; however, did not meet the criteria for selection in any of the groups.

2) MBR Limits

Provide MBR Limits for those items that met selection for the SCl or SC3 file, but did not meet selection for any of the group criteria.

f. Office of Quality Performance (OQP) Test Material - **Deliver to ORSIS for OQP**

To assist OQP in studying the results of the **Current Year (CCYY)** Mid-Year Mailing Operation the following materials are requested.

All test record listings generated for the following samples should use the Record Specification format contained in Attachment 1.

The following OQP listings, 1) through 4), should be delivered to ORSIS. See number 5 below for additional instructions.

NOTE: BOTH THE 2% ROUNDUP AND MONTHLY SAMPLES WILL CONTAIN ONLY THOSE RECORDS WHOSE SSN ENDS IN EITHER "02" OR "44".

l) For the 2 percent random sample of all the roundup selection groups provide:

o a test record listing, in duplicate using both the CSDOCAA7 and CSDOCHH7 files and,

o one set of corresponding MBR limits using CSLIMTFF (for the selected account numbers).

2) All the records selected in each of the continuing monthly selections beginning with the August selection and continuing through the October selection. This listing must be in segment/CAN order, rather than the ZIP CODE order required by the vendor.

3) For the 1/10 of 1 percent, CATF sample file provide:

o test record listing for all records, whose SSN ends in 05, 20, 45, 70 or 95, selected in the initial roundup selection.

(CSONEREC)

o one set of corresponding MBR limits

(CSLIMTDD)

4) For records selected meeting groups 14 and 15 criteria provide:

o a test record listing (CSDOCII4) using the Record Specification in Attachment 1 and

o MBR LIMITS (CSLIMTCC) matching the selected records.

5) Copy of the DOC file and the MBR file from both the roundup and monthly production runs to Jerry Kuhn.

2. Continuing Monthly Selection (August-October)

a. Monthly CSMY.WDOC File

Create the OLBG.BTI.CSMY.WDOC and OLBG.BTI.CSMY.WDOC.S files in accordance with item C.l.a.1) above. Send one copy of the file to Wilkes-Barre DOC.

b. CSMY.WDOB File

The OLBG.BTI.WB2.CSMYWDOB.RYYMMDD file must contain all 9781 records selected during the monthly runs in August, September and October.

c. ZIP CODE Listing

Produce the ZIP CODE (CSWDOCZP), only using five digit zip, listing in the same manner described in C.l.b. above.

d. Test Record Listing and LIMITS (CSDOCHH4 - 1/10 of 1%), (CSLIMTDD - 1/10 OF 1% LIMIT), (CSDOCII4 GROUPS 14 AND 15), (CSLIMTCC - GROUPS 14 & 15 LIMIT), (CSDOCAA7 AND CSDOCHH7 - 2 %), (CSLIMTFF 2% LIMIT) AND (CSLIMTF2 - FALLOUT LIMITS).

Produce a print listing in accordance with item C.l.c.2) above; however, print all the selected records.

e. Totals

Produce the totals report as outlined in (C.1.d.1) above.

3. Vendor Mailed Notices – Fill-ins for SSA-L9778 SUP, SSA-L9779 SUP, SSA-L9781 SM, SSA-L9784 SM and SSA-L9785 SM.

The following documents the fill-ins required for the above notices. The information provided is to assist the vendor in preparing the notices. The required data should be extracted from the tape files utilizing the Record Specification on Attachment 1. These requirements are also in conjunction with the notices maintained by OPBP.

a. SSA-L9778 SM-SUP Notice

l) Letter - Page 1 – fill-ins

a) Beneficiary Name
b) Beneficiary Address with Advanced POSTNET Barcode
c) CAN
d) BIC
e) Amount of Reported Earnings (AORE)

2) Instructions – Page 1 – fill-ins

a) Beneficiary name
b) CAN
c) BIC

3) Instructions - Page 2 – fill-ins

a) Month (Month spelled out) of FRA attainment

b) Year of FRA attainment (CCYY)

4) Questionnaire - Page 1 – fill-ins

a) Beneficiary Name
b) CAN
c) BIC
d) MM/YY
e) MM/YY
f) AORE

5) Questionnaire - Page 2 – fill-ins

None

Exhibit J – Mailer 3 & 4 – MYM

6) Questionnaire - Page 3 – fill-ins

None

b. SSA-L9784 SM Notice

l) Letter - Page 1 – fill-ins

a) Beneficiary Name

b) Beneficiary Address with Advanced POSTNET Barcode

c) CAN

d) BIC

2) Letter - Page 2 – fill-ins

None

3) Questionnaire - Page 1 – fill-ins

a) Beneficiary Name

b) CAN

c) BIC

d) MM/YY

e) MM/YY

f) Month (spelled out)

4) Questionnaire - Page 2 – fill-ins

None

5) Questionnaire - Page 3 – fill-ins

None

c. SSA-L9779 SM-SUP

l) Letter - Page 1 – fill-ins

a) Beneficiary Name

b) Beneficiary Address with Advanced POSTNET Barcode

c) CAN

d) BIC

e) AORE

2) Instructions – Page 1 – fill-ins

a) Beneficiary name

b) CAN

c) BIC

Exhibit J – Mailer 3 & 4 – MYM

3) Instructions - Page 2 – fill-ins

a) Month (month spelled out) FRA attainment
b) Year of FRA attainment (CCYY)

4) Questionnaire - Page 1 – fill-ins

a) Beneficiary Name
b) CAN
c) BIC
d) MM/YY
e) MM/YY
f) AORE
g) NonWork Months (NWM)

5) Questionnaire - Page 2 – fill-ins

None

6) Questionnaire - Page 3 – fill-ins

a) Beneficiary Name
b) CAN
c) BIC

7) Questionnaire - Page 4 – fill-ins

None

d. SSA-L9785-SM

1) Letter - Page 1 – fill-ins

a) Beneficiary Name
b) Beneficiary Address with Advanced POSTNET Barcode
c) CAN
d) BIC

2) Letter - Page 2 - fill-ins

None

3) Questionnaire - Page 1 - fill-ins

a) Beneficiary Name
b) CAN
c) BIC
d) MM/YY
e) MM/YY
f) Month (spelled out)

4) Questionnaire - Page 2 - fill-ins

NonWork Months

5) Questionnaire - Page 3 - fill-ins

a) Beneficiary Name
b) CAN
c) BIC

6) Questionnaire - Page 4 - fill-ins

None

e. SSA-L9781 SM

l) Coversheet - Page 1 - fill-ins

a) Beneficiary Name
b) Beneficiary Address with Advanced POSTNET Barcode
c) CAN
d) BIC
e) AORE

2) Instructions – Page 1 – fill-ins

a) Beneficiary name
b) CAN
c) BIC

3) Instructions - Page 2 - fill-ins

a) Month (Month spelled out) FRA attainment

b) Year of FRA attainment (CCYY)

4) Questionnaire - Page 1 - fill-ins

a) Beneficiary Name
b) CAN
c) BIC
d) MM/YY
e) MM/YY
f) AORE
g) NonWork Months (NWM)

5) Questionnaire - Page 2 - fill-ins

None

6) Questionnaire - Page 3 - fill-ins

a) Beneficiary Name
b) CAN
c) BIC

7) Questionnaire - Page 4 - fill-ins

None

D. <u>Edit Criteria</u>

Appropriate selection/edit criteria, requested by the user are specified in this request.

E. <u>Security/Privacy</u>

No changes to Special Security of Special Privacy requirements are called for in this request.

Exhibit J – Mailer 3 & 4 – MYM

SUMMARY

DATE	**PAGE #**	**EXPLANATION OF CHANGE**
03/15/Current Year (CCYY)		Updated the functional requirements to reflect the CURRENT YEAR (Current Year (CCYY)) and the FUTURE YEAR (Prospective Year (Current Year + 1)). Updated the functional requirements with CURRENT YEAR Earnings ($AORE) for beneficiaries under FRA and ($37680) for beneficiaries ≥ FRA.
10/22/10	14	Updated the functional requirements to call the SNO database to obtain the SNO Code, telephone number and SNO Priority Code for beneficiaries, applicants, recipients and representative payees who are blind or visually impaired.

Exhibit J – Mailer 3 & 4 – MYM

FILE CHARACTERISTICS FOR THE ANNUAL EARNINGS TEST MID-YEAR MAILING VENDOR TAPE FILES CSMY.WDOC

Recording Medium	TSILO
Record Length	**340**
Block Length	**29,920**
Record Format	Fixed Block
Label Type	IBM Standard
Recording Density	38K BPI
Recording Mode	EBCDIC
Parity	Odd

Record Sequence:

1. Notice Number

   (The notice number sequence is: 9778S, 9779S, 9781, 9784 and 9785

2. ZIP Code

3. CAN

4. BIC

Internal File Name:

CSMY.WDOC

External File Name: CSMY.WDOC

Exhibit J – Mailer 3 & 4 – MYM

File Characteristics for the Annual Earnings Test Mid-Year Mailing DOC Non-Responder Files
CSMY.WDOB

Record Medium	Magnetic Tape
Record Length	30
Block Length	600
Record Format	Fixed Block
Label Type	IBM Standard
Recording Density	1600 BPI
Recording Mode	EBCDIC
Parity	Odd

Record Sequence:

CAN
BIC
DOB

Internal File Names:

CSMY.WDOB

External File Name:

CSMY.WDOB

1.0 General Information

A. Project Abstract

The class action, American Council of the Blind v. Astrue, requires SSA to offer two additional special notice options to applicants, beneficiaries, recipients, and representative payees who are blind or visually impaired.

B. Organizational Information

Organization Preparing Document

ORSIS, DT2NM, NAB, Renee K. Stancil,
IT Specialist, 4-H-10 Operations, Ext. 6-9494

Organization Requesting Document

DCO, Mary Glenn-Croft, Deputy Commissioner for Operations

Organization Responsible for Validation/Acceptance

ORSIS, DT2NM, NAB, Renee K. Stancil,
IT Specialist, 4-H-10 Operations, Ext. 6-9494

ORSIS, DT2NM, NDB, Djimy Chapron
Branch Chief, 4-H-11 Operations, Ext 6-9402

2.0 Processing Requirements

A. Scope/Overview

Currently the NCOA process does not offer blind beneficiaries any options of how they would like to receive their notices. SSA will now offer these beneficiaries the special notice options of receiving their letters by regular mail, regular mail with supplementary contact by telephone, certified mail, in Braille, on a compact disc (CD) in Microsoft Word format, on an Audio CD, or in Large Print. A template of each type of NCOA notice will now be stored in ORS.

B. Inputs

Special Notice Option (SNO) Database
MBR – REPD
TOP
RPNI
RPN

C. Outputs

Two regular files will be created for the print vendor
OLBG.BTI.CDCI.NCOA.S1.RYYMMDD
OLBG.BTI.CDCI.NCOA.S2.RYYMMDD

Two certified mail files will created for transmission to the print vendor
OLBG.BTI.CDCI. NCOA.S1.CERT.RYYMMDD
OLBG.BTI.CDCI. NCOA.S2.CERT.RYYMMDD

Four blind files will be created for transmission to WBDOC
OLBG.BTI.WBD.SNORSPCP.NCOAE1.RYYMMDD
OLBG.BTI.WBD.SNORSPCP.NCOAS1.RYYMMDD
OLBG.BTI.WBD.SNORSPCP.NCOAE2.RYYMMDD
OLBG.BTI.WBD.SNORSPCP.NCOAS2.RYYMMDD

Four blind files will be created for transmission to the SNO vendor
OLBG.BTI.NTI.SNORSPRD.NCOAE1.RYYMMDD
OLBG.BTI.NTI.SNORSPRD.NCOAS1.RYYMMDD
OLBG.BTI.NTI.SNORSPRD.NCOAE2.RYYMMDD
OLBG.BTI.NTI.SNORSPRD.NCOAS2.RYYMMDD

NOTE: Do not transmit any empty files

D. Detailed Functional Analysis

See attached specs

E. Service Level Requirements

No changes

F. Security and Privacy

No changes

3.0 Logical Data Requirements

No change

4.0 Validation Plan

SNO R2.2/T2_R20 (February 2011) Release

Detailed Functional Requirements

1. General Specifications

Paper Size – 8 ½ x 11
Margins – Side 1 inch
Top ½ inch
Type Size – Text – Upper/lower case Century Schoolbook in 12-point medium
Captions – 12-point bold
Headings – Line 1 - 18-point medium, upper and lower case
Line 2 – 18-point bold, upper and lower case
Line 3 – 14-point medium, upper and lower case
Spacing of text – Single spaced with double spacing to separate paragraphs, captions from text, or blocks of information.
Printing – 2 sided
Margins – ½ inch at top and bottom of page. 1 inch left side. Right margin not justified.

2. Placement of Fixed Data

Captions – flush to left margin
Captioned Text – begins 1/8 inch from left margin
Bullets – place ¼ inch from left margin
"AND" or "OR" – when used between bullets, place ¾ inch from left margin
"See Next Page" - centered on bottom line of first page of multi-page notices
Field Office Address in Referral Paragraph – 3 ½ inches from left margin
Signature Block – begins at the center of the 5th line after end of text
Enclosures – listed flush to left margin 2 lines after signature

Headings

The heading will be printed beginning ½ inch from the top of the page and 1 inch from the left side of the page.

The first line of the heading will be "Social Security Administration" printed in 18-point medium.

The second line of the heading will be "Retirement, Survivors and Disability Insurance" printed in 18 point bold.

The third line of the heading will be "Important Information" printed in 14-point medium.

3. Placement of Variable Data

Date

The word “Date” (Fecha) followed by a colon will be printed beginning 4 ⅝ inches from the left side and 1 ¾ inches from the top of the page. The month will be either March (marzo), June (junio), September (septiembre), or December (diciembre), depending on the quarterly run.

** The notice date will be forwarded in the files that are transmitted to WBDOC and NTIS in the format 03/18/2011 (mm/dd/ccyy). It will have to be converted to word form listed above (English and Spanish) for any printed notices.*

Claim Number

The words “Claim Number” (Número de Reclamación) followed by a colon will be printed directly under the date. The claim number will be the Record ID Number derived from positions 01-09 of the variable data followed by a space and the one or two positions PIC (payment identification code) derived from positions 10-11 of the variable data.

Mailing Address

The mailing address will be printed beginning 2 ½ inches from the top of the page at the left margin.

The mailing address consists of the Payee name as shown in positions 285-372 of the variable data, the street address derived from positions 478-517, and the city, state, and zip code from positions 518-541.

NOTE: If a nine position zip is available, all nine digits will be shown on th**e** notice.

The postal barcode will be printed directly under the city, state, and zip code.

The postal barcode is derived by combining the 9-position ZIP code in positions 533-541 and the ZIP Delivery Point Code (ZDPC) derived from positions 542-544 of the variable data.

The vendor will be responsible for converting this data into a barcode suitable for mailing.

NOTE: The vendor may adjust the positioning of the address in the window of the envelope as needed to allow for correct clearances.

Text Content

There are 4 different notices to be printed.

Form SSA-L292-SM (MM/YY)	Exhibit-B
Form SSA-L292-SM-SP (MM/YY)	Exhibit-C
Form SSA-L294-SM (MM/YY)	Exhibit-D
Form SSA-L294-SM-SP (MM/YY)	Exhibit-E

Exhibits B, C, D, and E included in this document show the text, captions, headings, etc. for each notice.

NOTE: The exhibits show everything to be printed. However, they are not printed according to the specifications in this document.

Category and Type of Notice To Be Sent

There are 2 categories of notices. Each category will have a English and Spanish version of the notice. **The vendor will need to read position 276 of the variable data for each record to determine if a Spanish notice is needed**. Position 276 will contain a “S” if the beneficiary elects to have written correspondence in Spanish.

Category 1

The beneficiaries selected for this category will receive either Form SSA-L-292-SM (MM/YY) for English speaking beneficiaries or Form SSA-L-292-SM-SP (MM/YY) for Spanish speaking beneficiaries. The variable data for these beneficiaries will be contained in the file
OLBG.BTI.CDCI.NCOA.S1.RYYMMDD.
OLBG.BTI.CDCI. NCOA.S1.CERT.RYYMMDD

Category 2

The beneficiaries selected for this category will receive either Form SSA-L-294-SM (MM/YY) for English speaking beneficiaries or Form SSA-L-294-SM-SP (MM/YY) for Spanish speaking beneficiaries. The variable data for these beneficiaries will be contained in the file
OLBG.BTI.CDCI.NCOA.S2.RYYMMDD.
OLBG.BTI.CDCI. NCOA.S2.CERT.RYYMMDD

4. Variable Data Within the Text

The variable data within the body of the text will consist of the fill-ins necessary to complete the referral paragraph under the caption **“If You Have Any Questions.”**

There are 4 variations of this paragraph depending on the variable data fields present on the record. The variable data fields to be used in determining which variation to use are:

DO Phone Number – Positions 778-789
DO Street Address – Positions 680-745
DO City, State, Zip – Positions 746-777

Variation 1

Language - English

If you have any questions, you may call us toll-free at 1-800-772-1213, or call your local office at (1). We can answer most questions over the phone. You can also write or visit any Social Security office. The office that serves your area is located at:

(2)

PLEASE DO NOT WRITE TO THE RETURN ADDRESS SHOWN ON THE ENVELOPE. If you do call or visit an office, please have this letter with you. It will help us answer your questions.

Language – Spanish

Si tiene preguntas, puede llamarnos gratis al 1-800-772-1213, o llamas a su oficina local de Seguro Social al (1). Podemos contestar la mayoría de sus preguntas por teléfono. También puede escribir o visitar cualquier oficina del Seguro Social. La oficina que sirve su área está ubicada en:

(2)

POR FAVOR NO ESCRIBA A LA DIRECCION DE REMITENTE EN EL SOBRE. Si llama o visita una oficina, por favor tenga esta carta consigo. Nos ayudara a contestar sus preguntas.

Usage

Variation 1 will be used if the DO phone number in positions 778-789 of the variable data contains **other than** 800-772-1213 or blank.

AND

The DO address in position 680-777 **is not** blank.

Fill-ins

Fill-in (1) will consist of the DO phone number from positions 778-789.

Fill-in (2) will be the DO address from positions 680-777
Variation 2

Language - English

If you have any questions, you may call us toll-free at 1-800-772-1213. We can answer most questions over the phone. You can also write or visit any Social Security office. The office that serves your area is located at:

(1)

PLEASE DO NOT WRITE TO THE RETURN ADDRESS SHOWN ON THE ENVELOPE. If you do call or visit an office, please have this letter with you. It will help us answer your questions.

Language – Spanish

Si tiene preguntas, puede llamarnos gratis al 1-800-772-1213. Podemos contestar la mayoría de sus preguntas por teléfono. También puede escribir o visitar cualquier oficina del Seguro Social. La oficina que sirve su área está ubicada en:

(1)

POR FAVOR NO ESCRIBA A LA DIRECCION DE REMITENTE EN EL SOBRE. Si llama o visita una oficina, por favor tenga esta carta consigo. Nos ayudara a contestar sus preguntas.

Usage

Variation 2 will be used if the DO phone number in positions 778-789 is 800-772-1213 **or** blank

AND

The DO address in positions 680-777 **is not** blank.

Fill-ins

Fill-in (1) will consist of the DO address from positions 680-777.

<u>Variation 3</u>

<u>Language - English</u>

If you have any questions, you may call us toll-free at 1-800-772-1213, or call your local Social Security office at (1). We can answer most questions over the phone. If you do call an office, please have this letter with you. It will help us answer your questions.

<u>Language – Spanish</u>

Si tiene preguntas, puede llamarnos gratis al 1-800-772-1213, o llamas a su oficina local del Seguro Social al (1). Podemos contestar la mayoría de sus preguntas por teléfono. Si decide llamar a una oficina, por favor tenga esta carta consigo. Nos ayudará a contestar sus preguntas.

<u>Usage</u>

Variation 3 will be used if the DO phone number in positions 778-789 contains **<u>other</u> <u>than</u>** 800-772-1213 or blank

AND

The DO address in positions 680-777 **<u>is</u>** blank.

<u>Fill-ins</u>

Fill-in (1) will consist of the DO phone number from positions 778-789.

<u>Variation 4</u>

<u>Language - English</u>

If you have any questions, you may call us toll-free at 1-800-772-1213. We can answer most questions over the phone. If you do call, please have this letter with you. It will help us answer your questions.

<u>Language – Spanish</u>

Si tiene preguntas, puede llamarnos gratis al 1-800-772-1213. Podemos contestar la mayoría de sus preguntas por teléfono. Si decide llamar a una oficina, por favor tenga esta carta consigo. Nos ayudará a contestar sus preguntas.

Usage

Variation 4 will be used if the DO phone number in positions 778-789 is 800-772-1213 **OR** blank

AND

The DO address in positions 680-777 **is** blank.

Fill-ins

None

5. Signature Requirements

The Assistant Regional Commissioner Processing Center Operations (ARCPCO) signature or the Office of Central Operations (OCO) Executive's signature, printed name and title will appear on the last page of the notice. The placement of this data will vary and is directly related to the last line of the notice text. The signature data will never be placed on a page by itself and must be preceded by at least 3 lines of text on the same page.

The signature data consists of 4 lines of information. The first line will be the ARCPCO's or OCO Executive's signature; the second line will be the ARCPCO's, OCO's printed name; the third line will be the title "Assistant Regional Commissioner" or "Associate Commissioner for"; the fourth line will be "Processing Center Operations" or "Central Operations".

1. Develop First Line of Signature

   - Placement – The first line will be printed directly above the ARCPCO's printed name and will be 4 ¼ inches from the left edge of the page. (Approximately print position 43)

   - Print Type – Digitized script. The vendor will be provided with the digitized signature

   - Content – The facsimile of the ARCPCO's signature.

2. Develop Second Line of Signature Data

- Placement – The second line will be printed on the sixth line below the last line of the notice text (begin printing on the sixth line) and will be 4 ¼ inches from the left edge of the page (approximately print position 43).

- Print Type – 12-point medium density

- Content – Printed Name

3. Develop Third Line of Signature Data

- Placement – The third line will be placed directly under the second line of the signature data and will be 4 ¼ inches from the left edge of the page (approximately print position 43).

- Print Type – 12-point medium density

- Content – The third line will contain the title "Assistant Regional Commissioner" or "Associate Commissioner for".
  Spanish – "Comisionada Regional Asistente,
  Comisionado Regional Asistente, or
  Comisionada Associada de."

4. Develop Fourth Line of Signature Data

- Placement – The fourth line will be placed under the third line of the signature data and will be 4 7/16 inches from the left edge of the page (approximately print position 45)

- Print Type – 12-point medium density

- Content – The fourth line will contain the phrase "Processing Center Operations" or "Central Operations".
  Spanish – "Operaciones del Centro de Procesamiento or
  Operaciones Centrales."

Insert the signature block based on the PSC number displayed in position 275 of the record layout.

PSC	**Notice**	**Signature Block**
1	L292SM	(**Digitized Signature**)
	L294SM	Anne Jacobosky
		Assistant Regional Commissioner
		Processing Center Operations
	L292SM-SP	(**Digitized Signature**)
	L294SM-SP	Anne Jacobosky
		Comisionada Regional Asistente
		Operaciones del Centro de Procesamiento
2	L292SM	(**Digitized Signature**)
	L294SM	Elaine Garrison-Daniels
		Assistant Regional Commissioner
		Processing Center Operations
	L292SM-SP	(**Digitized Signature**)
	L294SM-SP	Elaine Garrison-Daniels
		Comisionada Regional Asistente
		Operaciones del Centro de Procesamiento
3	L292SM	(**Digitized Signature**)
	L294SM	Quittie C. Wilson
		Assistant Regional Commissioner
		Processing Center Operations
	L292SM-SP	(**Digitized Signature**)
	L294SM-SP	Quittie C. Wilson
		Comisionado Regional Asistente
		Operaciones del Centro de Procesamiento
4	L292SM	(**Digitized Signature**)
	L294SM	Phyllis M. Smith
		Assistant Regional Commissioner
		Processing Center Operations
	L292SM-SP	(**Digitized Signature**)
	L294SM-SP	Phyllis M. Smith
		Comisionada Regional Asistente
		Operaciones del Centro de Procesamiento
5	L292SM	(**Digitized Signature**)
	L294SM	Hy Hinojosa
		Assistant Regional Commissioner
		Processing Center Operations

L292SM-SP (**Digitized Signature**)
L294SM-SP Hy Hinojosa
Comisionado Regional Asistente
Operaciones del Centro de Procesamiento

6 L292SM (**Digitized Signature**)
L294SM Lynn Marten
Assistant Regional Commissioner
Processing Center Operations

L292SM-SP (**Digitized Signature**)
L294SM-SP Lynn Marten
Comisionado Regional Asistente
Operaciones del Centro de Procesamiento

7/8 L292SM (**Digitized Signature**)
L294SM Terry Stradtman
Associate Commissioner for
Central Operations

L292SM-SP (**Digitized Signature**)
L294SM-SP Terry Stradtman
Comisionado Associada de
Operaciones Centrales

6. Notices

Undeliverable notices will be returned to the address on the mail-out envelope, currently Social Security Administration, 6401 Security Blvd, Baltimore, MD 21235-6401. NCOA returned mail is discarded.

7. <u>Determine Blind Notice Process</u>

Blind beneficiaries are provided the option of receiving notices by other than regular mail. The options are:

- Certified mail
- Contact by telephone
- Braille
- CD with WORD
- Other
- Audio CD
- Large Print

If the beneficiary elects to have certified mail, the Special Notice Option code will be "**1**". The "CERTIFIED MAIL" does not require a duplicate notice. However, it will be placed in a separate blind file.
If the beneficiary elects telephone contact, the Special Notice Option code will be " **2**". For "TELEPHONE CONTACT", a duplicate notice will be created and placed in a "blind" file for special handling.
If the beneficiary elects to have Braille, the Special Notice Option code will be "**3**". The notice will be produced in duplicate with a copy placed in the SNO Notice File.
If the beneficiary elects the MS WORD CD, the Special Notice Option will be a "**4**". The notice will be produced in duplicate with a copy placed in the SNO Notice File.
If the beneficiary elects Audio CD, the Special Notice Option code will be "**6**". The notice will be produced in duplicate with a copy placed in the SNO Notice File.
If the beneficiary elects Large Print, the Special Notice Option will be a "**7**". The notice will be produced in duplicate with a copy placed in the SNO Notice File.

A. <u>Function Logic</u>

Call the SNO UTILITY to obtain SNO data associated on either a COSSN/CID or CAN/BIC.

For situations where Rep Payee data exists on the MBR (REPD-IND=Y), RPNI = '1' and TOP ≠ A, and a RPN is present, call the SNO database using the RPN.

If the rep payee is an individual, REPD-IND = Y, RPNI = '1', and TOP ≠ A, but the RPN is blank, **do not call** SNO, send regular mail.

If Rep Payee data exists on the MBR, REPD-IND=Y and the Rep Payee Number is **NOT** an individual, (RPNI ≠ 1), **do not call** SNO, send via regular mail.

If Rep Payee data does **NOT** exist on the MBR (REPD-IND≠Y) **or**
Payee data **DOES** exist on the MBR (REPD-IND=Y) and TOP = 'A',
call the database using CAN/BIC or BOAN of the beneficiary.

If a match is found on the SNO database and the SNO code = 1, then generate a record on the “CERTIFIED MAIL” Notice file. File will be transmitted to the print vendor.

If a match is found on the SNO database and the SNO code = 2, move the phone number on the SNO database to positions 374 – 383 on the record layout. Generate a record on the “blind” file for transmission to the PSC. Generate a duplicate record (without the phone number) on the regular mail file for transmission to the print vendor.

If a match is found on the SNO database and the SNO code = 3, 4, 6, or 7, generate 2 records, 1 record to the regular mail file and 1 record to the SNO file for transmission to the SNO vendor.

If a Spanish language indicator is present (LANG = S), and the SNO code = “1” or “2”, no English version of the notice will be created. If a Spanish language indicator is present (LANG = S), and the SNO code = “3, 4, 6 or 7”, only a Spanish version will be sorted to the SNO file (no English version will be created).

The SNO Vendor will add the following language at the top of each SNO (Braille, Data CD) notice.
<u>English version</u>:
We are sending this letter to you in both a standard print version and in the special format that you requested. You will receive them in separate envelopes.

<u>Spanish version</u>:
Le estamos enviando esta carta en ambas, una versión impresa de manera estándar y en el format especial que usted pidió. Las recibirá en sobres separados.

NOTE: NCOA only generates completed notices.

B. <u>Notice Counts</u>

In addition, generate a count of the number of SNO transactions in a run. This count should be by SNO option, in a format similar to the one below, and available upon request.

Certified	(SNO Code = 1)	99
Telephone	(SNO Code = 2)	99
Braille	(SNO Code = 3)	99
Data CD	(SNO Code = 4)	99
Audio CD	(SNO Code = 6)	99
Large Print	(SNO Code = 7)	99
Total SNO Notices		999
Total Input for SNOFILE		
	(SNO Codes = 3, 4, 6 & 7)	999

C. ORS Template

For the purpose of reading the Telephone Contact notices, copies of the SSA-L292-SM, L292-SM-SP, L294-SM, and L294-SM-SP will reside on the ORS Mass Mailing website at: http://orsstd.sspf.ssa.gov/orsstd/search.do?foldername=MASS+MAIL&MASS+MAILING_operand=1&MASS+MAILING_value1=MASSM&POSTING+DATE_operand=1&POSTING+DATE_value1=07%2F31%2F00

Record Layout

SSA Record 1 - 400

Position	Length	Description
01-09	09	Record ID Number (SSN)
10-11	02	Payment Identification Code (PIC)
12-99	88	PNAL 1 – 4 (Payment Name Legend)
100-187	88	ADDR-ADRLN1 - 4 (street address)
188-207	20	ADDR-CITY (City)
208-209	02	ADDR-STATE (State)
210-218	09	ADDR-ZIP-PLUS4 (Zip Code + Zip + 4)
219-221	03	ADDR-ZDPC (Zip Delivery Point Code)
222-223	02	LAF
224-231	08	ADDR-UPDDT (Mailing Address Update Date)
232	01	ADDR-NUM-ADDRLN (Number of Mailing Address Lines)
233	01	Direct Deposit Code (DDCO)
234	01	Type of Payee (TOP)
235-244	10	Beneficiary First Name (BFN)
245	01	Beneficiary Middle Initial (BMI)
246-257	12	Beneficiary Last Name (BLN)
258-259	02	Beneficiary Identification Code (BIC)
260-265	06	Date of Susp or Term (DOST-mmddyy)
266	01	SSI Code (SISC)
267-274	08	Date of Birth (DOB-mmddccyy)
275	01	Payment Center (PSC)
276	01	Language
277-284	08	NCOA Selection Date (mmddccyy)
285-306	22	PNAL - 1
307-328	22	PNAL - 2
329-350	22	PNAL - 3
351-372	22	PNAL – 4
373-373	01	SNO Code*
374-383	10	Beneficiary Phone Number **
384-384	01	Priority Code ***
385-394	10	Notice Date (in format mm/dd/ccyy) ****
395-400	06	Filler

* obtained from SNO database

** obtained from SNO database for records with SNO Code =2 (will be used only by the WBDOC)

*** for future use

**** for use with the files sent to WBDOC and NTIS only (date will be derived from yearly approved schedule from OPLM)

NCOA Standard Address 401 - 477

Position	Length	Description
401-450	50	USPS Street Address
451-463	13	USPS City
464-465	02	USPS State
466-474	09	USPS Zip
475-477	03	USPS Zip Delivery Point Code

NCOA Update Information 478-552

Position	Length	Description
478-517	40	NCOA Street Address
518-530	13	NCOA City
531-532	02	NCOA State
533-541	09	NCOA Zip
542-544	03	NCOA Zip Delivery Point Code
545-552	08	USPS Change Effective Date

SSA Additions After Match 553-800

Position	Length	Description
553	01	Letter Type Indicator
554-556	03	DOC #1 (original)
557-561	05	State and County Code
562-583	22	DO Address Line 1
584-605	22	DO Address Line 2
606-627	22	DO Address Line 3
628-647	20	DO City
648-649	02	DO State
650-659	10	DO Zip
660-671	12	DO Phone Number
672-674	03	DO Code #2 (new)
675-679	05	State and County Code
680-701	22	DO Address Line 1
702-723	22	DO Address Line 2
724-745	22	DO Address Line 3
746-765	20	DO City
766-767	02	DO State
768-777	10	DO Zip
778-789	12	DO Phone Number
790-800	11	Filler

Social Security Administration

Retirement, Survivors and Disability Insurance

Important Information

Date: February 1, 2004
Claim Number: XXX-XX-XXXX XX

PAYEE NAME
AND ADDRESS
(UP TO 6 LINES)
POSTAL BARCODE

We are writing about your mailing address. The United States Postal Service has told us that they have a mailing address for you that is different from the mailing address on our records.

What You Need To Do

The mailing address the Post Office gave us is shown above. If you told us about this new address within the last 45 days, you can ignore this letter and you do not need to contact us.

If you did not tell us about this address, and the address is correct, **you do not need to contact us**. We will change your mailing address on our records in about 30 days from the date of this letter.

If you do not want us to use this address, or the address is not correct, please call us at the number shown below.

If You Have Questions

If you have any questions, you may call us toll-free at 1-800-772-1213, or call your local Social Security office at XXX-XXX-XXXX. We can answer most questions over the phone. You can also write or visit any Social Security office. The office that serves your area is located at:

STREET ADDRESS
CITY, STATE XXXXX-XXXX

PLEASE DO NOT WRITE TO THE RETURN ADDRESS SHOWN ON THE ENVELOPE.
If you do call or visit an office, please have this letter with you. It will help us answer your questions.

Signature
Title

Form **SSA-L292-SM** (MM-YYYY)

Administración de Seguro Social
Seguro de Jubilación, Sobrevivientes e Incapacidad
Información Importante

Fecha: 1 de febrero de 2004
Número de Reclamación: XXX-XX-XXXX XX

PAYEE NAME
AND ADDRESS
(UP TO 6 LINES)
POSTAL BARCODE (IF APPLICABLE)

Le estamos escribiendo con relación a su dirección postal. El Servicio Postal de los Estados Unidos nos ha informado que tiene una dirección postal para usted que es diferente a la que aparece en nuestros registros.

Lo que necesita hacer

La dirección postal que la Oficina de Correos nos dió aparece arriba. Si usted nos informó de esta nueva dirección dentro de los últimos 45 días, puede ignorar esta carta y no tiene que comunicarse con nosotros.

Si no nos informó de esta dirección, y la dirección está correcta, **no tiene que comunicarse con nosotros**. Cambiaremos su dirección postal en nuestros registros dentro de 30 días de la fecha que aparece en esta carta.

Si no quire usar esta dirección o la dirección no está correcta, favor de llamarnos al número de teléfono que aparece a continuación.

Si tiene preguntas

Si tiene preguntas, puede llamarnos gratis al 1-800-772-1213, o llamar a su oficina local del Seguro Social al XXX-XXX-XXXX. Podemos contestar la mayoría de sus preguntas por teléfono. También puede escribir o visitar cualquier oficina del Seguro Social. La oficina que sirve su área está ubicada en:

STREET ADDRESS
CITY, STATE XXXXX-XXXX

POR FAVOR NO ESCRIBA A LA DIRECCION DE REMITENTE EN EL SOBRE. Si llama o visita una oficina, por favor tenga esta carta consigo. Nos ayudará a contestar sus preguntas.

Signature
Title

Social Security Administration

Retirement, Survivors and Disability Insurance

Important Information

Date: February 1, 2004
Claim Number: XXX-XX-XXXX XX

PAYEE NAME
AND ADDRESS
(UP TO 6 LINES)
POSTAL BARCODE

We are writing about your mailing address. The United States Postal Service has told us that they have a mailing address for you that is different from the mailing address on our records.

What You Need To Do

The mailing address the Post Office gave us is shown above. If you told us about this new address within the last 45 days, you can ignore this letter and you do not need to contact us.

If you did not tell us about this address, but the address is correct, **please call us toll free at 1-800-772-1213.** We need to confirm the address before we begin using it.

If You Have Questions

If you have any questions, you may call us toll-free at 1-800-772-1213, or call your local Social Security office at XXX-XXX-XXXX. We can answer most questions over the phone. You can also write or visit any Social Security office. The office that serves your area is located at:

STREET ADDRESS
CITY, STATE XXXXX-XXXX

PLEASE DO NOT WRITE TO THE RETURN ADDRESS SHOWN ON THE ENVELOPE. If you do call or visit an office, please have this letter with you. It will help us answer your questions.

Signature
Title

Form **SSA-L294-SM** (MM-YYYY)

Administración de Seguro Social

Seguro de Jubilación, Sobrevivientes e Incapacidad

Información Importante

Fecha: 1 de febrero de 2004
Número de Reclamación: XXX-XX-XXXX XX

PAYEE NAME
AND ADDRESS
(UP TO 6 LINES)
POSTAL BARCODE (IF APPLICABLE)

Le estamos escribiendo con relación a su dirección postal. El Servicio Postal de los Estados Unidos nos ha informado que tiene una dirección postal para usted que es diferente a la que aparece en nuestros registros.

Lo que necesita hacer

La dirección postal que la Oficina de Correos nos dió aparece arriba. Si usted nos informó de esta nueva dirección dentro de los últimos 45 días, puede ignorar esta carta y no tiene que comunicarse con nosotros.

Si no nos informó de esta dirección, pero la dirección está correcta, **favor de llamarnos gratis al 1-800-772-1213.** Necesitamos confirmar la dirección antes de comenzar a usaría.

Si tiene preguntas

Si tiene preguntas, puede llamarnos gratis al 1-800-772-1213, o llamar a su oficina local del Seguro Social al XXX-XXX-XXXX. Podemos contestar la mayoría de sus preguntas por teléfono. También puede escribir o visitar cualquier oficina del Seguro Social. La oficina que sirve su área está ubicada en:

STREET ADDRESS
CITY, STATE XXXXX-XXXX

POR FAVOR NO ESCRIBA A LA DIRECCION DE REMITENTE EN EL SOBRE.
Si llama o visita una oficina, por favor tenga esta carta consigo. Nos ayudará a contestar sus preguntas.

Signature
Title

Form **SSA-L294-SM-SP** (MM-YYYY)

Exhibit J – Mailer 7 – 9 – Step Parent

REQUEST FOR OPERATIONAL SUPPORT

ANNUAL NOTIFICATION OF STEPPARENTS

A. BACKGROUND

This service request documents the processing necessary to generate annual notices for beneficiaries to notify SSA when a divorce from a stepparent becomes final.

The stepparent record will consist of 3 files (Domestic, Spanish and Foreign). The domestic, Spanish language and foreign files will be sorted in ZIP Code sequence. In addition, it will be necessary to access the DOORS data base to obtain district office address data which will appear in the notice for domestic and Spanish notices. See 1.0.A. for further information.

This is the layout of the file, generated by RETAP, that will be sent to CDCI.

Record Specification

ANNUAL NOTIFICATION OF STEPPARENTS

Record Length = 281   Block Size = 29,786

Record Location	Field Name	Program Mnemonic	Field Size	Foot Note
1-11	Account Number (includes dashes (-)	CAN	11	B
12-13	Beneficiary Identification Code	BIC	2	C
14-145	Beneficiary Name & Address (6 lines of up to 22 characters each)	PNA	132	D
146-150	5-digit Zip Code	ZIP	5	E
151-154	Zip +4	+4	4	F
155-157	Zip Point Delivery Code	ZDPC	3	G
158-171	Barcode Representation (*999999999999* or spaces)		14	H
172-183	District Office (DO) Phone (Format: XXX-XXX-XXXX)		12	I
184-205	DO Address Line 1		22	J
206-227	DO Address Line 2		22	K
228-249	DO Address Line 3		22	L
250-269	DO City		20	M

270-271	DO State	2	N
272-281	DO Zip Code (XXXXX-XXXX)	10	O

B. **PROCESSING-Specifications**

Record Identification:

Select if:

- M-TAC CD) does not equal ‘S’ (claim is not survivor)

  AND

- BIC = "A" with the first position of LAF =

  a. "A", "D", "P" (except PT), "S" or "E"

  OR

  b. "C" AND:
  M-ADVFILING-SW equals Y

  AND

- the account has a BIC "C" present on record with 1st position of LAF not equal to T, N, PT, U or W.

  AND

- CREL – TYPE = S
  AND CREL – ENDRSN NOT PRESENT.

The file that is returned from CDCI will prompt the creation of an intermediate file, which will have 381 characters in it. This will get the information from the SNO database:

Record Location	Field Name	Program Mnemonic	Field Size	Foot Note
1-11	Account Number (includes dashes (-)	CAN	11	B
12-13	Beneficiary Identification Code	BIC	2	C
14-145	Beneficiary Name & Address (6 lines of up to 22 characters each)	PNA	132	D

146-150	5-digit Zip Code	ZIP	5	E
151-154	Zip +4	+4	4	F
155-157	Zip Point Delivery Code	ZDPC	3	G
158-171	Barcode Representation (*999999999999* or spaces)		14	H
172-183	District Office (DO) Phone (Format: XXX-XXX-XXXX)		12	I
184-205	DO Address Line 1		22	J
206-227	DO Address Line 2		22	K
228-249	DO Address Line 3		22	L
250-269	DO City		20	M
270-271	DO State		2	N
272-281	DO Zip Code (XXXXX-XXXX)		10	O
282	SNO CODE		1	
283	SNO Priority Code		1	
284-298	Beneficiary or Rep Payee’s phone number		15	
299-369	Filler		71	
370-378	Rep Payee SSN		9	
379	Payment Center no-Office Code		1	
380-381	Language indicator		2	

The Payment Center Code and the language indicators are on this file to help sort the notices

Files:

1. Create files as follows:

   a. Foreign -- if M-FRGNPAY-SW=Y, there is a foreign address.

   b. Spanish -- if BIC "A" has Spanish language code (LANG = "S") and M-FRGN-SW is blank.

   c. Domestic -- if not a. or b. above, for domestic.

2. Four notice files with the same record format will be produced (See Attachment A):

   a. Stepparent Notice
      English (SSA-L253-SM)
      CSTP253E.RYYMMDD
      (English)

   b. Stepparent Notice
      Spanish (SSA-L253-SM-SP)
      CSTP253S.RYYMMDD
      (Spanish)

   c. Stepparent Notice
      Foreign (SSA-L253-SM-F)
      CSTP253F.RYYMMDD
      (Foreign)

   d. Stepparent Notice
      Certified Mail

There would be two files created for the certified mail- one for English and one for Spanish language. These files would be sent to the print vendor-CDCI-who handles the regular mailing. As of this writing, Foreign mail is not sent via certified mail. The print vendor will also get the '0' SNO indicators. See SNO EXTRACTION area below for details for creating the files.

SNO EXTRACTION

A call is made to the SNO data base. Each CAN in the SNO data base has a SNO indicator that designates what Special Notice Option applies. If the SNO indicator is '0', it means that no Special Notice Option is on file and that a regular notice is to be sent. If the SNO indicator is a '1', a '1' will be moved to space 282 of the step parent record (see Record Specification at the end of this document). A '1' in this space indicates the notice will be sent, via certified mail, to the address listed for the CAN on the stepparent notice record. If the SNO indicator on the SNO data base is a '2', a '2' will be moved to the step parent record. '2' in this space indicates that the notice will be sent, via first class mail to the address listed for the CAN on the stepparent notice record. In addition, a follow up phone call will be made. For the 2010 mailing, OAS will handle the phone call. In the future, a phone call center will be established in Wilkes-Barre to handle the phone calls. There is a space on the

Record Specification for the beneficiary’s phone number. This phone number is the one that is on the SNO data base. A ‘3’in the SNO indicator field will be moved to space 282: it means that a Braille notice must be sent to the address for the beneficiary. A ‘4’ in the SNO indicator will be moved to space 282: means that a data CD must be sent to the beneficiary. Future values for Space 282 are ‘5’ for other, ‘6’ for audio CD and ’7’ for large print notice. These are already on the SNO data base, but they are not in use, yet.

The print vendor who handles the regular stepparent notices(CDCI)will get the file with the SNO indicator of ‘1’.

CDCI will get the SNO indicators of ‘2’. OAS will handle the phone call this year. NTIS will get the SNO indicators of ‘3’ and ‘4’, as well as those of ‘5’, ‘6’ and ‘7’, when they become operational.

```
For each record identified and selected:
If Rep Payee Data exists on the Post MBR
          (REPD-IND = ‘Y’)
     and a Rep Payee exists (RPNI = ‘1’ and TOP ≠ ‘A’)
     and a RPN exists, access the SNO database
          using the RPN
else if Rep Payee Data exists on Post MBR
          (REPD-IND = ‘Y’)
     and a Rep Payee exists (RPNI = ‘1’ and TOP ≠ A’)
     and a RPN does not exist, do not access the
          SNO database and generate a record on the Regular
          Notice file
else if Rep Payee Data exists on the Post MBR
          (REPD-IND = ‘Y’)
     and Rep Payee Data exists (RPNI = ‘1’ and TOP = ‘A’)
          access the SNO database using the CAN/BIC or
          BOAN of the beneficiary
else if Rep Payee Data exists on the Post MBR
          (REPD-IND = ‘Y’)
     and a Rep Payee does not exist (RPNI ≠ ‘1’),
          do not access the SNO database and generate a
          record on the Regular Notice file
else if Rep Payee Data does not exist on the Post MBR
          (REPD-IND ≠ ‘Y’), access the SNO database
          using the CAN/BIC or BOAN of the beneficiary.
```

Exhibit J – Mailer 7 – 9 – Step Parent

```
If a match is found on the SNO database and the
     SNO Code equals ‘1’ generate a record on the Certified
     Notice file
else if a match is found on the SNO database and the
     SNO Code equals (‘3’ or ‘4’ or ‘6’ or ‘7’) move the
     SNO Code to the SNO Indicator,  generate a record
     on the SNO Notice file and generate a duplicate
     record, without the SNO Code, on the Regular Notice
     file
else if a match is found on the SNO database and
     the SNO Code equals ‘2’
     move the SNO Phone Number to the Telephone Contact,
     generate a record on the Blind Notice file and
     generate a duplicate record, without the Telephone
     Contact, on the Regular Notice file
else if a match is not found on the SNO database
generate a record on the Regular Notice file If the SNO
Code equals ‘2’, use the domestic phone number. If the
domestic phone number doesn’t exist use the foreign
phone number else move spaces to the Telephone Contact.
```

DOORS Match Operation:

This operation will use the domestic and Spanish language stepchild files from RETAP as input.

If domestic or Spanish, the district office phone number and address must be obtained from the DOORS database.

Exceptions to the DOORS match will be handled by creating a listing titled "Exception List - Stepparent" in the following format:

```
"EXCEPTION LIST - STEPPARENT"

SSN                      PNA
```

Perform the match as follows:

1. If the district office code (DOC) = blanks, do not access the DOORS data base and do NOT build a notice record. Add beneficiary (BIC "A") account number and PNA of the record to "Exception List - Stepparent".

2. If the DOC = last 3 positions of the DOC on the DOORS data base:

   a. If district office phone number is present, move this phone number to the stepchild record (DO Phone - positions 172-183).

b. If district office phone number is not present, move spaces to the stepchild record (DO Phone -positions 172-183).

c. If the office physical location is present, move this address to the Stepchild record (DO Address Information positions 184-281).

c. If the office physical location is not present, move blanks to the Stepchild record (DO address information positions 184-281).

2. If the DOC not = last 3 positions of DOC on DOORS data base, do not build a notice record. Add beneficiary (BIC "A") account number and PNA of record to "Exception List - Stepparent"

Sorting:

Create six files:

1. If domestic, sort files by ZIP +4 (9-digit ZIP code) in ascending order.
(CSTP253E.RYYMMDD)

2. If Spanish, sort files by ZIP +4 (9-digit ZIP code) in ascending order.
(CSTP253S.RYYMMDD)

3. If foreign, sort file by ZIP Code (will be in Consular Office Code order)
in ascending order. (NOTE:APO/FPO
addresses will be in this file).
(CSTP253F.RYYMMDD)

4. Certified mail-English

5. Certified mail-Spanish

6. Certified mail-Foreign (tentative; foreign mail is not currently sent via Certified mail.

Special Instructions:

- Test files to be produced by November 30, 2010.
- Test files will be generated to the vendor. Notify Ken Renehan, ORSIS, MPB, extension 6-3422 when files are ready.
- Production files will be delivered to the vendor on or before December 14, 2010.

- Provide ORSIS, MPB with the total number of record counts selected by each category (i.e. Domestic, Spanish and Foreign).

C. **INPUTS**

Current MBR File
DOORS Data Base

D. **OUTPUT**

T1 bulk data for the Vendor (See Attachment A for Record Specification):

1. Stepparent Notice
   English (SSA-L253-SM)
   CSTP253E.RYYMMDD
   (English)

2. Stepparent Notice
   Spanish (SSA-L253-SM-SP)
   CSTP253S.RYYMMDD
   (Spanish)

3. Stepparent Notice
   Foreign (SSA-L253-SM-F)
   CSTP253F.RYYMMDD
   (Foreign)

4. Certified Mail file

5. Exception List - See E. DOORS Match Operation.

6. Test Files (11/30/10) - 3 files (Spanish, English & Foreign) of 100 records each to be sent to the vendor and full production files on 12/14/10.

E. **Service Level Requirements**

N/A

F. **Security and Privacy Requirements**

N/A

G. **Vendor Notice Validation Strategy**

In order to validate that the Vendor can create proper notices, a test file is sent in October and notices for review are returned to Ken Renehan 410-966-3422 DT2E, MPB.
NOTE: We are not validating the RETAP process. IVEN will not be used.

Vendor to produce printout of notice records (100 records to include English, Spanish and Foreign records).

Produce TRIDE/DOORS Exception Listing

Data Review

Validation listing will be reviewed by ORSIS, DT2E, MPB, Ken Renehan, extension 6-3422.

Coordination

- ORSIS, DT2E, MPB, Ken Renehan, G-J-4 WHR, extension 6-3422.
- DT2CQ, OSB, Henry Eiswert, extension 5-5296.
- OPLM, Frederick Scheer, extension 5-6543
- OPBP, Cynthia Mages, extension 57985 [Spanish language contact]

Size

Validation files- 100 records for each version.
Production files- Full selections of set criteria.

Schedule

Activity	**Component**	**Target Date**
Select Records for validation	T2OSB	10/20/10
Provide copy of test File on SEF for OSR	T2OSB	10/25/10
Produce test files (3) for contractor (i.e., 100 records for each file, i.e., English, Spanish and Foreign)	T2OSB	11/30/10
Produce validation Output for ORSIS review	Contractor	12/03/10
Provide test results to contractor	MPB	12/07/10
Provide contractor with production files	T2OSB	12/14/10

Exhibit J – Mailer 7 – 9 – Step Parent

Record Specification
ANNUAL NOTIFICATION OF STEPPARENTS

Record Length = 281   Block Size = 29,786

Record		Program	Field	Foot
Location	Field Name	Mnemonic	Size	Note
1-11	Account Number (includes dashes (-)	CAN	11	B
12-13	Beneficiary Identification Code	BIC	2	C
14-145	Beneficiary Name & Address (6 lines of up to 22 characters each)	PNA	132	D
146-150	5-digit Zip Code	ZIP	5	E
151-154	Zip +4	+4	4	F
155-157	Zip Point Delivery Code	ZDPC	3	G
158-171	Barcode Representation (*999999999999* or spaces)		14	H
172-183	District Office (DO) Phone (Format: XXX-XXX-XXXX)		12	I
184-205	DO Address Line 1		22	J
206-227	DO Address Line 2		22	K
228-249	DO Address Line 3		22	L
250-269	DO City		20	M
270-271	DO State		2	N
272-281	DO Zip Code (XXXXX-XXXX)		10	O
282	SNO indicator- 1,2,3,4,6 or 7		1	P
283	Priority Code		1	
284-298	Beneficiary’s or Rep Payee’s Phone number from SNO database		15	Q
299-381	Filler		83	

Exhibit J – Mailer 7 – 9 – Step Parent

Foot Notes/Field Definitions:

A. Date/Fecha

The vendor will need to put the date on all the Notices, for the last business day of the calendar year.
NOTE: The notices will all be dated for December -- The Spanish translation for December is "Diciembre".

B. Account Number

Account number of beneficiary
The record will show hyphens (-) normally associated with this data.

C. BIC

Beneficiary Identification Code (may be 1 or 2 positions)

D. Beneficiary Name and Address (6 lines of address of up to 22 characters each)

This is taken from PNA1-PNA6 on the MBR for PIC A. Ensure that spaces right fill records with less than 6 PNAs.

E. 5-Digit Zip Code

This is the 5-digit Zip Code associated with the address.
(Foreign -- if first 2 positions of Zip Code are spaces, make the whole Zip code spaces)

F. Zip +4

This is the +4 add-on that is associated with the Zip code.

Note: All records may not have a +4. If there is no +4, move spaces to this field.

G. Zip Point Delivery Code

This is the Zip Point Delivery Code.
(NOTE: This will not be shown on the notice -- it is part of the barcode). If there is no Zip Point Delivery Code, put spaces.

H. Barcode Representation

The POSTNET barcode representation will be produced on the record in the following format:

(*999999999999*)

1. Where the barcode font starts.....(*)

3. The actual 12 digits of the Zip Code Data (i.e., the 5-digit Zip (positions 146-150), the +4 (positions 151-154) and the Zip Point Delivery Code (positions 155-157))

3. Where the barcode font stops.....(*)

4. If only 5 or 9-digit Zip, do not print barcode.

NOTE: This will always be underneath the last line of the address and will only be on domestic and Spanish notices. The vendor will be responsible for converting the numerics into a barcode suitable for mailing.

I. District Office Telephone Number

The record will display the hyphens (-) normally associated with this data. (i.e., XXX-XXX-XXXX)

The district office phone number will always be present on domestic and Spanish notices.

NOTE: The District Office Address, City, State and Zip Code will appear on all Domestic and Spanish notices.

J. First Line of District Office Address

K. Second Line of District Office Address

L. Third Line of District Office Address

J, K, L = the address of the physical location of the district office extracted from the DOORS data base. Initialize this field to blanks before accessing the DOORS data base.

M. District Office City

The city of the district office extracted from the DOORS data base. Initialize this field to blanks before accessing the DOORS data base.

N. District Office State

The State of the district office extracted from the DOORS data base. Initialize this field to blanks before accessing the DOORS data base.

O. District Office Zip Code

XXXXX-XXXX (Zip Code +4)
The record shows hyphens normally associated with this data.

The ZIP Code and +4 of the district office extracted from the DOORS data base. Initialize this field to blanks before accessing the DOORS data base.

NOTE: The DO Zip code may not have a Zip +4. If there is no +4 for the DO, show spaces.

Exhibit J – Mailer 7 – 9 – Step Parent

P. SNO indicator –‘1’ indicates certified mail, ‘2’ indicates telephone contact, ‘3’ indicates a Braille notice will be sent, along with a first class print notice. ‘4’ indicates a Data CD will be sent, along with a first class print notice.

Q. Beneficiary’s telephone number-phone number from the SNO database. If there is a Representative Payee on the SNO database, the telephone number must be that of the Rep Payee. If no Rep Payee, the telephone number is the beneficiary’s phone number as given on the SNO database. The telephone number on the SNO database is preferred over the one on the MBR. The SNO database is more current than the MBR.

The files are sorted by zip codes. CDCI gets the English, Spanish and the Foreign files for SNO Codes 2-7. CDCI gets the English and Spanish files for SNO Codes 1. There is no provision for Certified Mail in the Foreign file.

NTIS gets the English, Spanish and Foreign files for SNO Codes 3, 4, 6, and 7.

EXHIBIT J – Mailer 10 & 11 – Fee Adjustment

A. Background

Authorized Organizational representatives are permitted to charge a fee for services. The amount charged is limited to 10% of the beneficiaries' payment amount, but no more than $**??*** for no DA/A involvement and $**??*** for DA/A involvement. The COLA is due 12/10 and all parties must be notified of the potential increase in the fee to be collected.

Due to the above, notices of this increase need to be sent to the Representative Payee and the Beneficiary/Recipient.

As of 8/10, there are approximately 1,200 Organizational Representatives approved to charge a fee and approximately 120,000 beneficiaries being charged a fee. The number of beneficiary letters sent will depend upon the COLA.

* The exact amount of the fee will not be known until the amount of the COLA is announced in 10/10.

B. Processing

1. Representative Payee notice:

From the RPS database RP record, select the RPs who have an:
RPIDQ = 9 numeric and alpha O, and
ORGFEEAPVL = Y and
NO date in the ORGFEESTP
NO date in the ORGZNSTPDT

2. Beneficiary notice:

a. For each Representative Payee selected in step 1, select each Beneficiary/Recipient that is linked to the RP record with an R3 record or a pending decision type 98 in the R2 record.

b. For each R2/R3 record selected, compare against the MBR/SSR to verify that the current entitlement status is "in pay" on the MBR/SSR.
What is in pay?
For T2: LAF = [C/D]
For T16: PSY = [C01]

c. For each record that meets the above criteria, we will check the MBR/SSR for the DA&A code:

d. For - T2 select MBR = DIB DATA LINE - last iteration, DAA field, Codes {X/Y/Z]

-T16 select SSR = CMPH LINE and the last iteration of the DA&A field, D field (DRUG-M), Codes [X/Y/Z]

For multiple entitlements, finding the indicator on any entitlement will count as one DA&A record.

Annotate the records found with the DA&A codes [X/Y/Z].

EXHIBIT J – Mailer 10 & 11 – Fee Adjustment

C. Output

Output files will be produced according to record specifications in Appendixes A and C.

1. Representative Payee notice:

The information for the payee name and address (#1-6) and Zip code on Appendix A will be obtained from the RP record and will consist of:

RPMLGD
RPMADDR
RPMCITY
RPMSTATE
RPMZIP5

Note: Exact fees are unknown until the 2005 COLA figures are released in October 2010. The new fee amounts will be parmed into the program.

2. Beneficiary/Recipient notice:

The information for the beneficiary name and address (#1-6) and Zip code on Appendix C, will be obtained from the R2 and R3 records and will consist of:

BCFNAM
BCLNAM
BCSFFX

If the name fields together exceed 22 bytes, build the name backwards; i.e., last name, and then as many letters of the first name as possible.

For the BN address, use the BCLCTNIDQ from the R1 to access the RP record and pull:

RPMADDR
RPMCITY
RPMSTATE
RPMZIP5

The notice fill ins will consist of:

Fill in #1 - BICID
Fill in #2 - (DAA max/min amount)

To determine the DA&A maximum/minimum amount, use the codes from the MBR/SSR:

[X/Y/Z] fill in = ??*
All other codes or low values (blanks),
fill in = ??*

*Note = Exact fill-in is unknown until the 2010 COLA figures are released.

EXHIBIT J – Mailer 10 & 11 – Fee Adjustment

RECORD SPECIFICATIONS -- BENEFICIARY/RECIPIENT NOTICE

(Form SSA-L251-SM)

Record Location	Field Name	Field Size	A/N/C	Foot Note
01 - 11	SSN (Fill-in #1)	11	N/C	(1)
12 - 33	Bene Name and Address 1	22	A/N/C	
34 - 55	Bene Name and Address 2	22	A/N/C	
56 - 77	Bene Name and Address 3	22	A/N/C	
78 - 99	Bene Name and Address 4	22	A/N/C	
100 - 121	Bene Name and Address 5	22	A/N/C	
122 - 143	Bene Name and Address 6	22	A/N/C	
144 - 148	Zip code	5	N	
149 - 150	Fill-in #2	2	N	
151 – 152	Region Code	2	A/N/C	

[A] = ALPHA

[N] = NUMERIC

[C] = CHARACTER

(1) Includes Hyphens

EXHIBIT J – Mailer 10 – 11 – Fee Adjustment

RECORD SPECIFICATIONS -- REPRESENTATIVE PAYEE NOTICE

(Form SSA-L252-SM)

Record		Field		Foot
Location	Field Name	Size	A/N/C	Note
01 - 22	Payee Name and Address 1	22	A/N/C	
23 - 44	Payee Name and Address 2	22	A/N/C	
45 - 66	Payee Name and Address 3	22	A/N/C	
67 - 88	Payee Name and Address 4	22	A/N/C	
89 - 110	Payee Name and Address 5	22	A/N/C	
111 - 132	Payee Name and Address 6	22	A/N/C	
133 - 137	Zip Code	5	A/N/C	
138 – 139	Region Code	2	A/N/C	

NOTE: $($$) amounts on this letter will be set amounts supplied to the Vendor as soon as they are known.

[A] = ALPHA

[N] = NUMERIC

[C] = CHARACTER