Program:	564-S							
Term:	Date of Award to March 31, 2026							
Title:	SSA Printing, Receiving, and Fulfillment Program							
			DCG ONE EAST		**NPC INC.**		**CURRENT CONTRACTOR**	
		BASIS OF	Upper Marlboro, MD		Claysburg, PA		NPC INC.	
ITEM NO.	DESCRIPTION	AWARD	UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**
I.	**PREPRESS OPERATIONS:**							
(a)	Digital Color Content proof.....per trim/page-size unit...							
(1)	**Up to and including 8-1/2 x 11"**	262	$25.00	$6,550.00	$1.25	$327.50	$1.25	$327.50
(2)	**Over 8-1/2 x 11" up to and including 17 x 11"**	12	$25.00	$300.00	$2.50	$30.00	$2.50	$30.00
(3)	**Over 17 x 11" up to and including 25-1/2 x 11"**	10	$25.00	$250.00	$3.75	$37.50	$3.75	$37.50
(b)	PDF Soft Proof (Any Size Product).....per file.....	240	$50.00	$12,000.00	$5.00	$1,200.00	$5.00	$1,200.00
(c)	System Timework.....per hour.....	5	$100.00	$500.00	$150.00	$750.00	$150.00	$750.00
II.	**PRINTING AND BINDING**							
1.	**Format A (5-1/2 x 8- 1/2" up to and including 8-1/2 x 11")**							
(a)	Cut Sheet Forms: Printing face only in one ink color, including binding.....per cut sheet.....							
(1)	**Makeready and/or Setup**	4	$175.00	$700.00	$95.53	$382.12	$70.80	$283.20
(2)	**Running Per 1,000 Copies**	12	$11.25	$135.00	$17.99	$215.88	$4.59	$55.08
(b)	Cut Sheet Forms: Printing face and back, in one ink color, including binding.....per cut sheet.....							
(1)	**Makeready and/or Setup**	15	$175.00	$2,625.00	$115.36	$1,730.40	$80.40	$1,206.00
(2)	**Running Per 1,000 Copies**	156	$11.25	$1,755.00	$5.19	$809.64	$4.69	$731.64
2.	Format B (Over 8-1/2 x 11" up to and including 17 x 11"):							
(a)	Cut Sheet Forms: Printing face only in one ink color, including binding.....per cut sheet.....							
(1)	**Makeready and/or Setup**	1	$175.00	$175.00	$170.93	$170.93	$70.80	$70.80
(2)	**Running Per 1,000 Copies**	7	$25.50	$178.50	$29.14	$203.98	$9.13	$63.91
(b)	Cut Sheet Forms: Printing face and back only in one ink color, including binding.....per cut sheet.....							
(1)	**Makeready and/or Setup**	5	$175.00	$875.00	$190.36	$951.80	$80.40	$402.00
(2)	**Running Per 1,000 Copies**	16	$25.50	$408.00	$63.74	$1,019.84	$10.23	$163.68
3.	Format C (Over 17 x 11" up to and including 25-1/2 x 11"):							
(a)	Cut Sheet Forms: Printing face and back only in one ink color, including binding.....per cut sheet.....							
(1)	**Makeready and/or Setup**	10	$175.00	$1,750.00	$354.72	$3,547.20	$186.00	$1,860.00
(2)	**Running Per 1,000 Copies**	2,889	$36.75	$106,170.75	$20.19	$58,328.91	$15.35	$44,346.15
4.	Format D (Over 8-1/2 x 11"):							
(a)	Booklet Forms: Printing in a single ink color, including binding.....per page.....							
(1)	**Makeready and/or Setup**	404	$175.00	$70,700.00	$6.79	$2,743.16	$6.79	$2,743.16
(2)	**Running Per 1,000 Copies**	1,302	$20.63	$26,860.26	$4.51	$5,872.02	$3.70	$4,817.40
5.	Format E (Over 8-1/2 x 11"):							
(a)	Fact Sheet Publications: Printing face only in two ink colors, including binding.....per fact sheet.....							
(1)	**Makeready and/or Setup**	23	$175.00	$4,025.00	$224.48	$5,163.04	$184.00	$4,232.00
(2)	**Running Per 1,000 Copies**	306	$11.25	$3,442.50	$17.81	$5,449.86	$14.60	$4,467.60

Program:	564-S							
Term:	Date of Award to March 31, 2026							
Title:	SSA Printing, Receiving, and Fulfillment Program							
			DCG ONE EAST		**NPC INC.**		**CURRENT CONTRACTOR**	
		BASIS OF	Upper Marlboro, MD		Claysburg, PA		NPC INC.	
ITEM NO.	DESCRIPTION	AWARD	UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**
(b)	Fact Sheet Publications: Printing face and back in two ink colors, including binding.....per fact sheet.....							
(1)	**Makeready and/or Setup**	126	$175.00	$22,050.00	$248.88	$31,358.88	$204.00	$25,704.00
(2)	**Running Per 1,000 Copies**	1,129	$11.25	$12,701.25	$19.03	$21,484.87	$15.60	$17,612.40
6.	Format F (7 x 8" flat):							
(a)	Leaflet Publications: Printing face and back in two ink colors, including binding.....per leaflet.....							
(1)	**Makeready and/or Setup**	6	$175.00	$1,050.00	$281.68	$1,690.08	$180.00	$1,080.00
(2)	**Running Per 1,000 Copies**	974	$13.82	$13,460.68	$11.93	$11,619.82	$9.78	$9,525.72
7.	Format G (10-1/2 x 8" flat):							
(a)	Leaflet Publications: Printing face and back in two ink colors, including binding.....per leaflet.....							
(1)	**Makeready and/or Setup**	18	$175.00	$3,150.00	$366.00	$6,588.00	$300.00	$5,400.00
(2)	**Running Per 1,000 Copies**	212	$13.82	$2,929.84	$21.44	$4,545.28	$17.57	$3,724.84
8.	Format H (14 x 8" flat):							
(a)	Leaflet Publications: Printing face and back in two ink colors, including binding.....per leaflet.....							
(1)	**Makeready and/or Setup**	25	$175.00	$4,375.00	$366.00	$9,150.00	$300.00	$7,500.00
(2)	**Running Per 1,000 Copies**	336	$18.66	$6,269.76	$25.05	$8,416.80	$20.53	$6,898.08
9.	Format I (17-1/2 x 8" flat):							
(a)	Leaflet Publications: Printing face and back in two ink colors, including binding.....per leaflet.....							
(1)	**Makeready and/or Setup**	28	$175.00	$4,900.00	$366.00	$10,248.00	$300.00	$8,400.00
(2)	**Running Per 1,000 Copies**	429	$27.65	$11,861.85	$34.32	$14,723.28	$28.13	$12,067.77
10.	Format J (21 x 8" flat):							
(a)	Leaflet Publications: Printing face and back in two ink colors, including binding.....per leaflet.....							
(1)	**Makeready and/or Setup**	6	$175.00	$1,050.00	$366.00	$2,196.00	$300.00	$1,800.00
(2)	**Running Per 1,000 Copies**	42	$41.47	$1,741.74	$38.55	$1,619.10	$31.60	$1,327.20
11.	Format K (24-1/2 x 8" flat):							
(a)	Leaflet Publications: Printing face and back in two ink colors, including binding.....per leaflet.....							
(1)	**Makeready and/or Setup**	3	$175.00	$525.00	$549.00	$1,647.00	$450.00	$1,350.00
(2)	**Running Per 1,000 Copies**	17	$41.47	$704.99	$80.39	$1,366.63	$65.89	$1,120.13
12.	Format L (3-1/2 x 8"):							
(a)	Booklet Publications: Printing in two ink colors, including binding.....per page.....							
(1)	**Makeready and/or Setup**	660	$175.00	$115,500.00	$37.99	$25,073.40	$31.14	$20,552.40
(2)	**Running Per 1,000 Copies**	22,228	$20.63	$458,563.64	$11.80	$262,290.40	$15.63	$347,423.64

Program:	564-S							
Term:	Date of Award to March 31, 2026							
Title:	SSA Printing, Receiving, and Fulfillment Program							
			DCG ONE EAST		**NPC INC.**		**CURRENT CONTRACTOR**	
		BASIS OF	Upper Marlboro, MD		Claysburg, PA		NPC INC.	
ITEM NO.	DESCRIPTION	AWARD	UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**
13.	Format M (5-1/4 x 8"):							
(a)	Booklet Publications: Printing in two ink colors, including binding.....per page.....							
(1)	**Makeready and/or Setup**	1,308	$175.00	$228,900.00	$31.14	$40,731.12	$31.14	$40,731.12
(2)	**Running Per 1,000 Copies**	34,908	$20.63	$720,152.04	$10.50	$366,534.00	$17.28	$603,210.24
III.	**PAPER: Per 1,000 Leaves**							
1.	Format A (5-1/2 x 8-1/2" up to and including 8-1/2 x 11" (flat)):							
(a)	White Writing (16-lb.)	2	$9.07	$18.14	$13.00	$26.00	$13.00	$26.00
(b)	White Writing (20-lb.)	67	$9.07	$607.69	$13.00	$871.00	$13.00	$871.00
(c)	Colored Writing (10-lb.)	7	$19.83	$138.81	$18.00	$126.00	$18.00	$126.00
(d)	White Ledger (44-lb.); or, at contractor's option, White Index (90-lb.)	93	$39.65	$3,687.45	$42.00	$3,906.00	$42.00	$3,906.00
2.	Format B (Over 8-1/2 x 11" up to and including 17 x 11" (flat)):							
(a)	White Writing (20-lb.)	22	$19.15	$421.30	$19.50	$429.00	$19.50	$429.00
3.	Format C (Over 17 x 11" up to and including 25-1/2 x 11" (flat)):							
(a)	White Writing (20-lb.)	2,889	$39.56	$114,288.84	$29.25	$84,503.25	$29.25	$84,503.25
4.	Format D (8-1/2 x 11"):							
(a)	White Writing (20-lb.) or, at contractor's option, White Uncoated Text (50-lb.)	336	$9.07	$3,047.52	$13.00	$4,368.00	$13.00	$4,368.00
(b)	Colored Writing (20-lb.) or, at contractor's option, Uncoated Color Text (50-lb.)	316	$19.83	$6,266.28	$18.00	$5,688.00	$18.00	$5,688.00
5.	Format E (8-1/2 x 11"):							
(a)	White Uncoated Text (60-lb.)	1,435	$10.93	$15,684.55	$19.75	$28,341.25	$19.75	$28,341.25
6.	Format F (7 x 8" (flat)):							
(a)	White Uncoated Text (60-lb.)	974	$10.93	$10,645.82	$13.50	$13,149.00	$13.50	$13,149.00
7.	Format G (10-1/2 x 8" (flat)):							
(a)	White Uncoated Text (60-lb.)	212	$10.93	$2,317.16	$19.75	$4,187.00	$19.75	$4,187.00
8.	Format H (14 x 8" (flat)):							
(a)	White Uncoated Text (60-lb.)	336	$25.16	$8,453.76	$24.88	$8,359.68	$24.88	$8,359.68
9.	Format I (17-1/2 x 8" (flat)):							
(a)	White Uncoated Text (60-lb.)	429	$25.36	$10,879.44	$27.65	$11,861.85	$27.65	$11,861.85
10.	Format J (21 x 8" (flat)):							
(a)	White Uncoated Text (60-lb.)	42	$27.92	$1,172.64	$34.83	$1,462.86	$34.83	$1,462.86
11.	Format K (24-1/2 x 8" (flat)):							
(a)	White Uncoated Text (60-lb.)	17	$27.92	$474.64	$46.10	$783.70	$38.70	$657.90
12.	Format L (3-1/2 x 8"):							
(a)	White Uncoated Text (60-lb.)	11,114	$4.69	$52,124.66	$13.82	$153,595.48	$13.82	$153,595.48
13.	Format M (5-1/4 x 8-1/2"):							
(a)	White Uncoated Text (60-lb.)	17,454	$7.06	$123,225.24	$15.80	$275,773.20	$15.80	$275,773.20

Program:	564-S							
Term:	Date of Award to March 31, 2026							
Title:	SSA Printing, Receiving, and Fulfillment Program							
			DCG ONE EAST		**NPC INC.**		**CURRENT CONTRACTOR**	
		BASIS OF	Upper Marlboro, MD		Claysburg, PA		NPC INC.	
ITEM NO.	DESCRIPTION	AWARD	UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**
IV.	**ADDITIONAL OPERATIONS:**							
(a)	Perforating/ Scoring:							
(1)	Makeready and/or Setup (each perforation or score).....per line.....	48	$75.00	$3,600.00	$20.00	$960.00	$20.00	$960.00
(2)	Running (Maximum 3 lines per run).....per 1,000 leaves.....	3,102	$5.00	$15,510.00	$1.00	$3,102.00	$1.00	$3,102.00
(b)	Drilling.....per 1,000 leaves.....	156	$5.00	$780.00	$1.50	$234.00	$1.50	$234.00
(c)	Shrink-wrapping.....per package.....	150,380	$0.39	$58,648.20	$0.64	$96,243.20	$0.52	$78,197.60
(d)	Storage of inventory.....per month.....	12	$15,000.00	$180,000.00	$10,000.00	$120,000.00	$10,000.00	$120,000.00
(e)	Picking items for fulfillment.....per individual fullfillment order.....	16,754	$7.00	$117,278.00	$29.15	$488,379.10	$18.72	$313,634.88
(f)	Destruction of sensitive material.....per 1,000 pieces.....	1	$500.00	$500.00	$20.00	$20.00	$20.00	$20.00
V.	**PACKING AND DISTRUBTION:**							
(a)	Single or multiple copies in kraft envelpe (up to 200 leaves).....per envelope.....	4,918	$10.00	$49,180.00	$3.50	$17,213.00	$2.00	$9,836.00
(b)	Single or multiple copies over 200 leaves, up to 12 pounds , in cushonied shipping bags, or wrapped in shipping bundles (maximum gross weight 14 pounds).....per bag or bundle...	25,871	$15.00	$388,065.00	$4.50	$116,419.50	$3.00	$77,613.00
(c)	Quantities over 12 pounds, up to 36 pounds, packed in shipping containers maximum gross weight 40 pounds.....per container.....	26,945	$20.00	$538,900.00	$5.50	$148,197.50	$4.00	$107,780.00
	CONTRACTOR SUBTOTALS			**$3,555,200.94**		**$2,498,416.01**		**$2,491,898.11**
	DISCOUNT		**0.25%**	$8,888.00	**0.25%**	$6,246.04	**0.25%**	$6,229.75
	DISCOUNTED TOTALS			**$3,546,312.94**		**$2,492,169.97**		**$2,485,668.36**
						AWARDED		

U.S. GOVERNMENT PUBLISHING OFFICE
Washington, DC

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

SSA Printing, Receiving, and Fulfillment Program

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

Social Security Administration (SSA)

Single Award

TERM OF CONTRACT: The base term of this contract is for the period beginning **Date of Award** (for April 2025) and ending **March 31, 2026**, plus up to four (4) optional 12-month extension period(s) that may be added in accordance with the "OPTION TO EXTEND THE TERM OF THE CONTRACT" clause in SECTION 1 of this contract.

The period from Date of Award (expected to be after April 1, 2025) through September 30, 2025, will be used by the contractor for installation of VPN, security clearance, programming, proofing, testing, and transferring of materials to the new production facility. Actual, live production begins on or around October 1, 2025.

NOTE: The purchase order issue date is not expected to have an effective "Term of Program" prior to April 1, 2025. No VPN installation, security clearances, programming, proofing, testing or transferring of materials to the new production facility , as required by these specifications, is allowed on this contract prior to April 1, 2025, or Date of Award. In the event that the purchase order is issued before April 1, 2025, the contract base term will begin April 1, 2025. The base term year may be for less than a full 12 months.

BID OPENING: Bids shall be opened virtually at 11:00 a.m., Eastern Time (ET), on **January 22, 2025**, at the U.S. Government Publishing Office. All parties interested in attending the bid opening shall email bids@gpo.gov one (1) hour prior to the bid opening date and time to request a Microsoft Teams live stream link. This must be a separate email from the bid submission. The link will be emailed prior to the bid opening.

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

RESTRICTION ON LOCATION OF PRODUCTION FACILITIES: All production facilities used in the manufacture, storage, and fulfillment of the products ordered under this contract must be located within a 250-mile radius of Baltimore, MD. (Refer to "BID RESTRICTIONS" specified on page 2 for additional information.)

BIDDERS, PLEASE NOTE*: Requirements for this program were previously procured under Program 730-S.* These specifications have been extensively revised; therefore, all bidders are cautioned to familiarize themselves with all provisions of these specifications before bidding, with particular attention to:

1) SECURITY REQUIREMENTS: Clause 2352.224-1; **2)** Clause 2352.224-2A; **3)** Clause 2352.204-1; **4)** Clause 2352.204-2; and **5)** SECTION 4. – SCHEDULE OF PRICES, BID ACCEPTANCE PERIOD.

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

For information of a technical nature, contact **David Love** at (202) 512-0104 or email dlove@gpo.gov.

SECTION 1. – GENERAL TERMS AND CONDITIONS

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

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

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

BID RESTRICTIONS: Bidders must have an established warehouse for storage and fulfillment *prior* to the bid opening date specified above in order to be eligible for award of this contract. This warehouse must be located within the restricted production area (see "RESTRICTION ON LOCATION OF PRODUCTION FACILITIES"). Bidders must provide the location of the warehouse in their bid (see "LOCATION OF WAREHOUSE").

NOTE: Any bidder who does not have a warehouse prior to the bid opening date and that is not located within the restricted production area will be declared non-responsive.

SUBCONTRACTING: The predominant production functions are the printing and binding of items with PII and the storage, fulfillment of all products, and destruction of PII materials, as required. Any bidder that cannot perform the predominant production functions will be declared non-responsible.

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

If the contractor plans to enter into a "Contractor Team Arrangement" or Joint Venture, to fulfill any requirements of this contract, they must comply with the terms and regulations as detailed in the Printing Procurement Regulation – (GPO Publication 305.3; Rev. 2-24).

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

Product Quality Levels:

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

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

(a) Non-destructive Tests - General Inspection Level I.
(b) Destructive Tests - Special Inspection Level S - 2.

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. Halftone Match (Single and Double Impression)	O.K. Press Sheet
P-9. Solid and Screen Tint Color Match	O.K. Press Sheet

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

P-7. O.K Proofs; Average Type Dimension in Publication; Electronic Media
P-8. O.K. Proofs; Electronic Media;
P-9. 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 be considered to include this clause, except, the total duration of the contract may not exceed five (5) years as a result of, and including, any extension(s) added under this clause. Further extension may be negotiated under the "EXTENSION OF CONTRACT TERM" clause. See also "ECONOMIC PRICE ADJUSTMENT" for authorized pricing adjustment(s).

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

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

For the purpose of this clause, performance under this contract will be divided into successive periods. The first period will extend from **Date of Award** to **March 31, 2026**, 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, 2024**, called the base index. The percentage change (plus or minus) of the variable index from the base index will be the economic price adjustment for the period being considered for adjustment.

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

If the Government exercises an option, the extended contract shall be considered to include this economic price adjustment clause.

NOTE: Economic price adjustments are not cumulative and are to be applied to original bid prices only.

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

NOTE: For the purpose of this contract, the Paper Price Adjustment will be based on the date of actual production. Actual (live) production begins October 1, 2025.

1. BLS code **0913** for *All Paper* will apply to all paper required under this contract.

2. The applicable index figures for the month of **September 2025**, will establish the base index.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A copy of this signed certification must be forwarded to: SSA, Attn: Matthew Thomas, DMIM, 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235-6401, or email to: Matthew.Thomas@ssa.gov. A copy must also be forwarded to: U.S. Government Publishing Office, 732 North Capitol Street, NW, CSAPS, APS DC, Attn: Contracting Officer, Room C-838, Washington, DC 20401 (email address to be provided after award). (See paragraph (f) below regarding the minimum standards that the safeguards must meet.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

f. All ESPs that process or store Personally Identifiable Information (PII) (as defined in Clause 2352.224-2A (a)) are considered a Moderate impact categorization. If PII or sensitive data (defined by the COTR) is stored or processed by the ESP, then the ESP shall provide a Security Authorization Package (SAP), which will undergo a Triannual Full Assessment and will undergo an Annual Review. The SAP should include a System Security Plan (SSP), Security Assessment Report (SAR), Risk Assessment Report (RAR), and Plan of Action & Milestone Report (POA&M).

The SAP must be reviewed by SSA before the SSA transfers data to the ESP. Refer to NIST SP 800-37 and NIST SP 800-53r5 (or later) for more information on the Security Authorization Package. (Refer to "SAFEGUARDING FEDERAL TAX INFORMATION REQUIREMENTS" if an independent assessor is needed to accomplish this requirement.)

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

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

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

- Federal Information Security Modernization Act (P.L. 113-283), December 2014.
  https://www.govinfo.gov/app/details/PLAW-113publ283
- Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996."
  https://www.govinfo.gov/content/pkg/USCODE-2011-title40/html/USCODE-2011-title40-subtitleIII.htm
- Privacy Act (P.L. 93-579), December 1974.
  https://www.govinfo.gov/app/details/STATUTE-88/STATUTE-88-Pg1896
- Homeland Security Presidential Directive 12 (HSPD-12): "Policy for a Common Identification Standard for Federal Employees and Contractors," January 27, 2022.
  https://www.dhs.gov/homeland-security-presidential-directive-12
- Revision of OMB Circular No. A–130, "Managing Information as a Strategic Resource," July 28, 2016.
  https://www.govinfo.gov/content/pkg/FR-2016-07-28/pdf/2016-17872.pdf
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," December 16, 2003.
  https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf
- ITL BULLETIN FOR DECEMBER 2011 REVISED GUIDELINE FOR ELECTRONIC AUTHENTICATION OF USERS HELPS ORGANIZATIONS PROTECT THE SECURITY OF THEIR INFORMATION SYSTEMS.
  https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul2011-12.pdf
- FIPS PUB 199, National Institute of Standards and Technology, Federal Information Processing Standards Publication, "Standards for Security Categorization of Federal Information and Information Systems," February 2004.
  https://doi.org/10.6028/NIST.FIPS.199
- FIPS PUB 200, National Institute of Standards and Technology, Federal Information Processing Standards Publication, "Minimum Security Requirements for Federal Information and Information Systems," March 2006.
  https://doi.org/10.6028/NIST.FIPS.200
- FIPS 140-3, "Security Requirements for Cryptographic Modules," March 22, 2019.
  https://csrc.nist.gov/publications/detail/fips/140/3/final
- NIST Special Publication (SP) 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems," February 2006.
  https://doi.org/10.6028/NIST.SP.800-18r1

- NIST SP 800-30, Revision 1, "Guide for Conducting Risk Assessments," September 2012. https://doi.org/10.6028/NIST.SP.800-30r1
- NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems," November 2010. https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2010-07.pdf
- NIST SP 800-37, Rev. 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
- NIST SP 800-47, Rev. 1, "Managing the Security of Information Exchanges," July 2021. https://csrc.nist.gov/News/2021/nist-publishes-sp-800-47-rev-1
- NIST SP 800-53, Rev. 5, "Security and Privacy Controls for Information Systems and Organizations," September 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
- NIST SP 800-53A, Revision 5, "Assessing Security and Privacy Controls in Information Systems and Organizations," January 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf
- NIST SP 800-60, Vol. 1, Rev. 1, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008. https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final
- NIST SP 800-60, Vol. 2 Rev. 1, "Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices," August 2008. https://csrc.nist.gov/publications/detail/sp/800-60/vol-2-rev-1/final
- OMB M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 2017.
- NIST 800-171, Rev. 3, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," May 2024. https://csrc.nist.gov/pubs/sp/800/171/r3/final

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

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

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

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

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

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

SECURITY WARNING:

All employees working on this contract must:

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

Contractor's managers working on this contract must:

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

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

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

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

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

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

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

(a) *Definitions.*

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

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

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

Some common examples of a breach include:

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

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

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

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

"Personally identifiable information" (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. The PII may range from common data elements such as names, addresses, dates of birth, and places of employment, to identity documents, Social Security numbers (SSN) or other government-issued identifiers, precise location information, medical history, and biometric records. Within this clause, "PII" shall specifically mean PII that is made or becomes available to the contractor, including its employees, as a result of performing under this contract.

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

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

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

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

(b) *Responsibility for Safeguarding PII.*

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

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

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

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

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

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

(c) *Safeguarding Requirements.*

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

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

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

(ii) The contractor shall ensure that its PII policies and procedures address transporting PII outside a secure area and emailing PII to and from non-SSA email addresses. The contractor shall provide employees, upon or immediately prior to their commencing work on the contract, with contact information and instructions relating to PII breaches and incidents, based on the contractor's security/PII loss incident policy and procedures.

(If the preceding requirement is introduced to the contract under a contract modification, the contractor shall ensure employees are provided this information and instructions within 10 working days of the modification.) The contractor shall periodically remind employees of the foregoing information and instructions per the regular training requirements at (d)(1) below. (NOTE: Agency-prescribed contact information and instructions for reporting lost or possibly lost PII are discussed in paragraph (d) below.) SSA may require that the contractor present evidence of compliance with these provisions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) *Procedures*.

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

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

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

(A) Contact information;

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

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

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

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

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

(G) Any other pertinent information.

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

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

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

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

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

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

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

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

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

(4) The contractor shall bear the cost for any data breach or incident: (1) occurring outside of SSA-controlled facilities, systems, or environments when the affected PII was in the possession or control of the contractor or its employees, agents, or representatives; or (2) resulting from the contractor or its employees, agents, or representatives' failure to properly safeguard PII or facilities, systems, or other environments containing PII in accordance with this contract's requirements.

In addition, as SSA requires, the contractor shall be responsible for or shall assist SSA in taking preventative and remedial actions that SSA determines are necessary to address such a breach or incident.

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

(f) *Subcontractor(s).*

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

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

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

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

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

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

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

SAFEGUARDING FEDERAL TAX INFORMATION REQUIREMENTS:

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

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

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

"Return" means any tax or information return, estimated tax declaration or refund claim required by or permitted

under the IRC and filed with the IRS by, on behalf of, or with respect to any person or entity.

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

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

I. PERFORMANCE

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

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

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

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

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

(5) The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to SSA.

When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide SSA with a statement containing the date of destruction, description of material destroyed, and the destruction method.

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

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

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

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

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

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

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

II. CRIMINAL/CIVIL SANCTIONS

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

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

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

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

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

III. INSPECTION

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

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

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

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

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

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

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

"CO" means contracting officer.

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

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

"COR" means contracting officer's representative.

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

"CSPS" means Center for Suitability and Personnel Security.

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

"NBIS" means National Background Investigation Services.

"PIV" means Personal Identity Verification.

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

(b) Purpose

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

PIV Credentials

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

(2) A PIV credential is not required for:

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

or

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

(c) Authorities

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

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

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

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

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

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

(d) Suitability Process

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

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

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

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

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

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

(1) Suitability Document Submission

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

(i) An Applicant Listing including the names of all applicants requesting suitability;

(ii) Completed Optional Form (OF) 306, Declaration for Federal Employment;

(iii) Proof of citizenship and/or work authorization documents for non-U.S. born applicants, if applicable.

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

The required suitability forms and a sample of properly completed forms are available on SSA's Office of Acquisition and Grants (OAG) website ("Information About Acquisitions" tab, "Security Information" section [https://www.ssa.gov/oag/acq/ASC_2352_204-1_Security_and_Suit_Reqrmts_Post_10012017/Links%20for%20Agency%20Specific%20Clause%2023522_204-1%20Post%2010012017.htm]).

(2) eApp Form and Fingerprint Submission

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

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

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

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

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

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

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

(3) Status Check

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

(e) Suitability Determination

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

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

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

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

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

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

(h) Unsuitable Determinations

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

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

dchr.ope.suitclarify@ssa.gov

OR

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

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

(i) Contractor Notification to Government

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

(j) Obtaining a Credential

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

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

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

(4) Contacts

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

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

(k) Contractor Return of PIV Credential

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

(l) Government Control

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

(m) Removal From Duty

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

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

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

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

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

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

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

(7) Improper use of official authority or credentials.

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

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

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

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

(12) Violation of security procedures or regulations.

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

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

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

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

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

Regional Security Offices and Regional Credentialing Contacts for Contractor Personnel:

Region 1 – Boston
Management and Operations Support, Wilson Osorio, (617) 565-2840

Region 2 – New York
Center for Materiel Resources, Physical Security and Safety Team, Emmanuel Fernandez, (212) 264-2603

Region 3 – Philadelphia
For Mid-Atlantic Social Security Center occupants: Center for Materiel Resources, Kevin Wiley, (215) 597-1627
For all others: Center for Automation, Security and Integrity, (215) 597-5100

Region 4 – Atlanta
Center for Security and Integrity
Willie Martin, (404) 562-1761
Charlene C. Jones, (404) 562-1432
Glen Gaston, (404) 562-1871
Dennis Loewer, (404) 562-1340

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
Colleen Carrington, (312) 575-5242

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

Region 7 – Kansas City
Center for Automation 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 Howard, (510) 970-4124

Region 10 – Seattle
Center for Security and Integrity
Mary Bates, (206) 615-2105
Lisa Steepleton, (206) 615-2183

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

Definitions

Terms defined for this clause:

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

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

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

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

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

(b) Agency Responsibility Related to FISMA Training Requirements

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

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

(c) Contractor Responsibilities Related to FISMA Training Requirements

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

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

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

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

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

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

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

(i) Following contract award, the contractor shall ensure that all contractor personnel performing under this contract take the security awareness training by reading and signing the CPSC form, SSA-222. This requirement also applies to contractor personnel subsequently added to the contract. A copy of this form is on OAG's Internet website (SSA-222) (See Exhibit G)

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

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

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

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

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

Email Procedures

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

To Encrypt a File using WinZip

i. Save the file to contractor's hard drive.

ii. Open Windows Explorer and locate the file.

iii. Right click on the file.

iv. Select "WinZip."

v. Select "Add to Zip File."

vi. An Add box pops up. Near the bottom of the box is an "Options" area.

vii. Click the "Encrypt added files" checkbox.

viii. Click the "Add" button.

ix. Check the "Hide Password" checkbox if not already checked.

a. Enter a string of characters as a password composed of letters, numbers, and special characters (minimum 8 characters – maximum 64 characters).

b. Select the 256-Bit AES encryption radio button.

c. Click "OK."

x. The file has been encrypted successfully, and the new Zip file can now be attached to an email.

Providing the Recipient with the Password

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

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

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

Sending an encrypted Zip File via email

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

PREAWARD SURVEY: In order to determine the responsibility of the prime contractor or any subcontractor, the Government reserves the right to conduct an on-site preaward survey at the contractor's/subcontractor's facility or to require other evidence of technical, production, managerial, financial, and similar abilities to perform, prior to the award of a contract. As part of the financial determination, the contractor in line for award may be required to provide one or more of the following financial documents:

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

The documents will be reviewed to validate that adequate financial resources are available to perform the contract requirements. Documents submitted will be kept confidential and used only for the determination of responsibility by the Government. Failure to provide the requested information in the time specified by the Government may result in the Contracting Officer not having adequate information to reach an affirmative determination of responsibility.

Additionally, the preaward survey will include a review of all subcontractors involved, along with their specific functions; and the contractor's/subcontractor's backup facility, quality control, computer system, material/inventory control, personnel, security control, production area, fulfillment/shipping, replenishment/receiving, 100% accountability, and disposal of waste materials plans as required by this specification.

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

PREAWARD PRODUCTION PLANS: As part of the preaward survey, the contractor must present, in writing, to the Contracting Officer within five (5) workdays of being notified to do so by the Contracting Officer or his/her representative, detailed plans for each of the below 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.

Additionally, the contractor must submit a Security Authorization Package (SAP), as required, within 10 workdays of request. The workday after notification to submit will be the first day of the schedule. If the Government requests additional information after review of the SAP, the contractor must submit the additional information within three (3) workdays of request.

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

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

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

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

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

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

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

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

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

Backup Facility: The failure to produce and distribute the products produced on this program in a timely manner would have an impact on the daily operations of SSA. Therefore, if for any reason(s) (act of God, labor disagreements, national emergency, pandemic, 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 for producing and distributing the products specified in this program. The backup facility must be operated by the contractor.

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.

NOTE: All terms and conditions of this contract will apply to the backup facility.

Quality Control Plan: 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 provision herein are met. Contractor must perform, or have performed, the process controls, inspections, and tests required to substantiate that the products provided under this contract conform to the specifications and contract requirements. The contractor will 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 plan will detail how the contractor will ensure that the correct address label with recipient's address will be matched with the inserts to that same recipient inside the package. The plan will monitor all aspects of the job, including material handling and mail flow, to assure the production and distribution of these items meet specifications and Government requirements. This plan must also include the Quality Control measures taken when inspecting items received by the contractor and how defects will be communicated back to SSA.

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.

Computer System Plan: This plan must explain in detail how the contractor will receive task order files for fulfillment and replenishments as well as how the contractor will transmit data files back to SSA.

Material Handling and Inventory Control: This plan shall explain in detail how the following materials will be handled; incoming raw materials; receiving SSA materials; work-in-progress materials; quality control inspection materials; temperature and humidity-controlled storage of sensitive materials (envelopes, decals, etc.); and all outgoing materials cleared for pickup. The plan must also include how the contractor will maintain accurate inventory of all stocked items.

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

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

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

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

The plan must contain at a minimum:

- How Government files (data) will be secured to prevent disclosure to a third party.
- How the disposal of waste materials will be handled. (See "*Disposal of Waste Materials*.")
- How all applicable Government-mandated security/privacy/rules and regulations as cited in this contract must be adhered to by the contractor and/or subcontractor(s).

- How contractors classified as Cloud Service Providers (CSP) will adhere to additional FedRAMP security control requirements. CSPs must have a security control assessment performed by a Third Party Assessment Organization (3PAO).
- The contractor shall submit a System Authorization Package (SAP) as described in the "SSA External Service Provider Security Requirements" section. The SSP, a part of this package, documents how the solution implements security controls in accordance with the designated FIPS 199 security categorization and the Minimum Security Requirements for Federal Information and Information Systems. This SSP requires the use of NIST SP 800-53 v4. The SAP should be completed by either an independent assessor or another Federal agency.

Production Area – For this plan, the contractor must provide a secure area(s) dedicated to the processing and storage of data for this SSA workload, either a separate facility dedicated to Fulfillment orders and associated data, or a walled-in limited access area within the contractor's existing facility. Access to the area(s) must be limited to security-trained employees involved in the Fulfillment orders and associated data produced under this contract.

Part of the Production Area Plan must include a floor plan detailing the area(s) to be used for the storage of fulfillment items and the secure area where fulfillments will be packaged and staged for pickup. The floor plan must also show existing walls, access doors, security camera placement, and equipment to be used in the printing and finishing of the replenishment items produced at the contractor's facility.

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

Fulfillment and Shipping Plan: This plan shall include how fulfillment task orders are received and processed at the contractor facility. The plan must also explain how the contractor will pick items from inventory, track them through an internal workflow, and ensure all requested items are shipped, reported as back-ordered, or reported as cancelled timely to the schedule.

The fulfillment plan must also detail how the contractor will determine the shipping method for each fulfillment order. A majority of fulfillment orders will ship via SSA's UPS account. The remaining orders will be shipped reimbursable USPS Priority Mail.

Replenishment and Receiving Plan: This plan shall include how replenishment task orders are received and processed at the contractor facility. The plan must also explain how the contractor will fulfill stock replenishments and receive items from other contractors to be used for fulfillment orders. This plan must also include the contractors Quality Control check of received items and how issues will be reported back to SSA.

100% Accountability Plan: The plan shall explain how the contractor will ensure accurate inventory counts, process and track order fulfillment, and replenishment of stock items. The Government requires that a strict quality control mechanism be in place during the entire production period. The contractor is required to design a quality control system that will track the fulfillment of items and record back-order (out of stock) items for later fulfillment. A recovery system is required to ensure all items are being fulfilled accurately. This control system must use a unique sequential number to aid in the recovery program which has to be maintained in order to recover any missing or damaged items.

Barcoding: Each packaged item must be labeled and barcoded. The barcode must contain information regarding the packaged contents and include at a minimum the Product ID, Edition Date, and quantity. This barcode will be used to scan items into inventory and to scan when pulled from inventory for fulfillment. This will allow the contractor to keep an accurate inventory count of stocked items as well as track items as they are pulled for fulfillment.

Fulfillment Tracking: Each item will be tracked independently to ensure that the entire requested quantity for each item is fulfilled for each request. Fulfillment tracking will be reported back to SSA via the daily Fulfillment Status Update Report, as specified under "DAILY FULFILLMENT STATUS UPDATE FILES." This report shall provide information back to SSA stating when an item is fulfilled, the volume that was fulfilled, the edition date of the fulfilled item (if applicable), and shipping/tracking information. The Fulfillment Status Report will also include items that are either on back order or that have been successfully cancelled. Cancelled items will no longer require fulfillment. Back order items will remain in the contractor's fulfillment queue until they are fulfilled, and the full quantity is reported back to SSA as fulfilled accurately.

Replenishment Tracking: Each replenishment item will be tracked independently to ensure that each replenishment item is printed or received and stocked for fulfillment. Replenishment tracking will be reported back to SSA via the daily Replenishment Status Update Reports, as specified under "DAILY REPLENISHMENT STATUS UPDATE FILES." This report will provide information back to SSA stating when an item has been printed or received and stocked for fulfillment.

Inventory Reporting: The contractor must provide a daily inventory report back to SSA stating what the inventory is for each stocked item. The report will be provided at the same time each day. SSA will use this report to initiate replenishment orders to the contractor so that back-order volumes remain at a minimum.

Disposal of Waste Material: For this plan, 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.

If the contractor selects shredding as a means of disposal, it is preferred that a cross-cut shredder (one-quarter inch screen or finer) be used. If a strip shredder is used, the strips must not exceed one-quarter inch. The contractor must provide the location and method planned to dispose of the material.

A subcontractor may be used for the disposal of waste materials that do not contain PII. When a subcontractor is used, the same information is required, as well as how the material will be transported from the contractor's plant to the subcontractor. The plan must include the names of all contract officials responsible for the plan and describe their duties in relationship to the waste material plan.

NOTE: Non-sensitive materials such as blank forms and SSA publications will not be required to meet the same standards of sensitive (PII) SSA records.

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

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

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

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

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

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

PREPRODUCTION MEETING: A preproduction meeting covering the printing, inserting, and distribution shall be held at the contractor's facility after award of the contract, but prior to production, to review the contractor's production plan and to establish coordination of all operations. Attending this meeting will be representatives from the GPO and SSA.

The contractor shall present and explain their final plan for both printing and shipping. The contractor shall be prepared to present detailed plans, including such items as quality assurance, materials handling, and inventory control. At the Government's option, the preproduction meeting may be held via teleconference. The Government reserves the right to waive the preproduction meeting.

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

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, 2026**, 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 will detail the daily volume of orders required for fulfillment. A print order (GPO Form 2511) will be issued for billing purposes, will be issued weekly, and will cover all daily task orders issued that week.

A print order or task order shall be "issued" upon notification by the Government for purposes of the contract when it is electronically transmitted or otherwise physically furnished to the contractor in conformance with the schedule.

REQUIREMENTS: This is a requirements contract for the items and for the period specified herein. Shipment/delivery of items or performance of work shall be made only as authorized by orders issued in accordance with the clause entitled "ORDERING." The quantities of items specified herein are estimates only and are not purchased hereby. Except as may be otherwise provided in this contract, if the Government's requirements for the items set forth herein do not result in orders in the amounts or quantities described as "estimated," it shall not constitute the basis for an equitable price adjustment under this contract.
Except as otherwise provided in this contract, the Government shall order from the contractor all the items set forth which are required to be purchased by the Government activity identified on page 1.

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

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

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

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

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

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

PRIVACY ACT

(a) The contractor agrees:

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

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

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

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

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

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

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

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

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

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

PAYMENT: Submitting all invoices for payment via the GPO fax gateway (if no samples are required), utilizing the GPO barcode coversheet program application, is the most efficient method of invoicing. Instruction for using this method can be found at the following web address:

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

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

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

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

SECTION 2. – SPECIFICATIONS

SCOPE: These specifications cover the production of various printed products requiring such operations as electronic prepress, printing, binding, construction, packing, storage, receiving, fulfillment, and distribution.

TITLE: SSA Printing, Receiving, and Fulfillment Program.

FREQUENCY OF ORDERS: SSA intends to submit a print order for replenishments and a print order for fulfillments weekly to the contractor. The Replenishment print order issued Monday will cover the replenishment requests reported completed via the daily status update file provided by the contractor for the previous week. The Fulfillment print order issued Monday will cover the daily fulfillment task orders transmitted to the contractor Monday through Friday the previous week.

A separate print order will be issued at the beginning of each month for the storage charge for the current month (for example, the print order issued on June 1st would be for the month of June).

The Government reserves the right to increase or decrease the number of items that could be included in task orders and number of items carried on this contract per year by 25% for both replenishment and fulfillment orders.

Initial Startup Print Orders: SSA will issue an initial print order prior to live production beginning to cover the cost of the transportation of some material from a warehouse location within a 250-mile radius of SSA's Headquarters (Baltimore, MD). SSA will issue another print order on or after **October 1, 2025** to transport any remaining stock from this same warehouse location to the contractor's facility once production has begun.

There will be two types of replenishments: Items to be produced by the contractor and items to be received by the contractor.

Replenishment Task Orders: As stock reaches a replenishment point, as determined by SSA, SSA will issue replenishment task orders to the contractor for those items. The replenishment task orders will be sent to the contractor daily and will state if an item(s) is to be printed or received. As part of the replenishment task orders, the contractor will be notified of any upcoming deliveries that they will receive and stock as fulfillment items.

The contractor will provide daily reports for completed replenishments that they either printed or received, and SSA will issue the weekly replenishment print orders based on those completed replenishments.

Fulfillment Task Orders: Task orders will be issued daily for fulfillment and distribution of items to SSA's customers. A daily task order will require approximately 20 to 120 individual fulfillment requests. Each fulfillment will require the contractor to pick, pack, and ship numerous items to SSA customers at an average of three (3) items per fulfillment. It is possible for some task orders to contain as little as one (1) fulfillment requirement during an off-duty period (e.g., task orders issued around Federal Holidays).

NOTE: There may be some days when a task order is not issued.

Print orders will be issued weekly to cover all task orders placed the previous week.

Number of Production Orders:

It is impossible to determine the number or frequency of orders which will be placed during the term of this contract. However, based on historical data, it is anticipated that approximately 1 to 5 replenishment requests will be placed each year for each item produced by the contractor via the replenishment task orders.

Based on usage of these materials, the contractor will be notified via the daily replenishment task orders from SSA of what materials to print and replenish. The replenishment task orders will identify the product, volume, and packing for each printed replenishment item.

QUANTITY: SSA will identify the number of copies for each item in the replenishment task orders.

It is anticipated that the quantity will be approximately 500 to 1,000,000 copies per item per task order. Majority of replenishment requests issued will be for 50,000 copies or less per item.

TRIM SIZES:

Cut Sheet Forms –

Format A: 5-1/2 x 8-1/2" up to and including 8-1/2 x 11" (flat).
Format B: Over 8-1/2 x 11" up to and including 17 x 11" (flat).
Format C: Over 17 x 11" up to and including 25-1/2 x 11" (flat).

Booklet Forms –

Format D: 8-1/2 x 11".

Fact Sheet Publications –

Format E: 8-1/2 x 11".

Leaflet Publications –

Format F: 3-1/2 x 8" (folded down from 7 x 8" flat size).
Format G: 3-1/2 x 8" (folded down from 10-1/2 x 8" flat size).
Format H: 3-1/2 x 8" (folded down from 14 x 8" flat size).
Format I: 3-1/2 x 8" (folded down from 17-1/2 x 8" flat size).
Format J: 3-1/2 x 8" (folded down from 21 x 8" flat size).
Format K: 3-1/2 x 8" (folded down from 24-1/2 x 8" flat size).

Booklet Publications –

Format L: 3-1/2 x 8".
Format M: 5-1/4 x 8".

NUMBER OF PAGES (Applies to all formats specified for each product):

Cut Sheet Forms – 1 leaf (face only or face and back) per form.
Booklet Forms – Approximately 8 to 32 pages per booklet.
Fact Sheet Publications – 1 leaf (face only or face and back) per publication.
Leaflet Publications – 1 leaf (face and back) per publication.
Booklet Publications – Approximately 8 to 48 pages per publication.

FULFILLMENT OF SSA CUSTOMER ORDERS: The contractor will receive fulfillment task orders daily, Monday through Friday, from SSA. On average, the contractor can expect to receive 50 customer orders per day with an average of 3 items per order. The contractor's task will be to process the fulfillment orders by picking items out of inventory stock, pack items, ship items, and provide feedback and tracking via daily Fulfillment Status Update reports.

Back Order Items: The contractor will be required to provide status back to SSA on any item that is on back order (not in stock). Back order status updates are due on the same schedule as the initial fulfillment. Once an item is available for fulfillment, the contractor will fulfill the back order item and provide an updated status on the item.

Cancelling Items From a Fulfillment Order: Cancelled items will be indicated in the fulfillment task orders. The contractor will be required to provide status back to SSA on any items that the contractor was requested to cancel. If an item cannot be cancelled because it is already shipped, then the contractor will provide the shipped status back to SSA.

FULFILLMENT OF SSA REPLENISHMENT REQUESTS: The contractor will receive replenishment task orders daily, Monday through Friday, from SSA.

The contractor's task will be to process these replenishment requests orders by printing and stocking items or receiving and stocking items listed in the replenishment task order. The contractor will be required to provide feedback via daily Replenishment Status Update reports.

GOVERNMENT TO FURNISH:

Contract Start-Up Specifications:

- Printed Items Specification Spreadsheet: This spreadsheet will include all specifications for all contractor-produced items that will be available for fulfillment.
- Initial Retrieving Stock Report: This report will outline all items that the contractor will be required to retrieve from a warehouse location within a 250-mile radius of SSA's Headquarters (Baltimore, MD), re-package, and label as necessary. These items will need to be stocked and ready for production start-up.
- Final Retrieving Stock Report: This report will outline all items remaining for the contractor to retrieve from a warehouse location within a 250-mile radius of SSA's Headquarters. This report will be provided after the production start-dates.

Daily Transmissions: Two (2) Microsoft Excel files will be furnished via the contractor-hosted SFTP server on a daily basis, Monday through Friday. One file will be the stock replenishment task order; the other file will be the fulfillment task order.

1. Stock Replenishment Task Order File (See Exhibit H):
   - The purpose of this task order file is to authorize the contractor to replenish stocked items.
   - The file will contain items that are both produced by the contractor and items that are scheduled to be received and stocked by the contractor.
   - The Stock Replenishment task order files will follow a standard format (See Exhibit H).
   - The contractor will be notified 20 workdays in advance of any file format changes.
   - Example of Excel Format Name: "Taskorder replenishment_YY####-#.xls" (YY####-# will be replaced with the actional task order number each day.

2. Fulfillment Task Order File (See Exhibit I):
   - The purpose of this task order file is to provide fulfillment information to the contractor.
   - This file will contain fulfillment request information from SSA's customers.
   - The contractor will use this file to package and ship items needed by SSA's customers.
   - The fulfillment task order files will follow a standard format (See Exhibit I) .
   - The contractor will be notified 20 workdays in advance of any task order format changes.
   - Example of Excel Format Name: "Taskorder fulfillment_YY####-#.xls" (YY####-# will be replaced with the actional task order number each day).

Furnished Inventory:

- ***Start-Up:*** The Government will furnish, and the contractor will stock, an initial inventory of items for contract start-up. These items will be identified to the contractor via the Initial Stock Retrieval Report (See Exhibit J). The furnished items will be staged for the contractor to pick up from a warehouse location within a 250-mile radius of SSA's Headquarters in Baltimore, MD. (See "CONTRACT START-UP AND TRANSFER OF INVENTORY.")

  Items to be furnished by the Government will include printed items and specialty items. Printed items will include current stock of printed forms and publications at SSA's warehouse facility. Specialty items will include, but are not limited to, envelopes, decals, publications packets, folders, posters, information cards, etc., at SSA's warehouse facility.

- ***Throughout Term of Contract:*** Based on usage of these materials, the contractor will be notified via the daily replenishment task orders from SSA of what items will be printed or delivered for receiving and stocking. The replenishment task orders will identify the product, volume, packing, edition date (if applicable), and arrival date the contractor can expect to receive an item.

NOTE: *Printed items are products that will be furnished for initial inventory and furnished throughout the term of the contract but may also be ordered for production by the contractor on this contract. Specialty items are items that will be furnished for initial inventory and furnished throughout the term of the contract. Specialty items will not be ordered for production by the contractor on this contract.*

Furnished Materials for Contractor-Produced Products: Electronic media for SSA's products will be provided upon contract award. The contractor must hold and re-use furnished materials to produce replenishments. In the event of a change to the furnished files, SSA will furnish new materials to the contractor. Once revised files are approved, the contractor will hold and re-use the new files.

Electronic media will be furnished as follows:

Platform: Macintosh OSX; IBM or compatible using MS Windows.

Storage Media: Contractor-hosted SFTP server; on occasion, CD-R/RW, DVD-R/RW, or email.

Software: Adobe Creative Suite (InDesign, Photoshop, and Illustrator); Adobe Acrobat Professional with LiveCycle Designer; and Adobe Experience Manager (AEM).

NOTE: All files will be created in current versions or near current versions of the above mentioned programs.

All platform system and software upgrades (for specified applications) which may occur during the term of the contract must be supported by the contractor. The contractor must provide the upgrades within one (1) month of notification by the Government.

Fonts: All printer and screen fonts will be furnished/embedded, as applicable. All fonts used for this contract will be Adobe Type I and/or TrueType.

The contractor is cautioned that the furnished fonts are the property of the Government and/or its contractors. All furnished fonts are to be eliminated from the contractor's archive immediately after completion of the contract.

Additional Information: Files will be furnished in PostScript, native application, and/or PDF format.

Electronic media will include all illustrations and graphics furnished in place.

Visuals of electronic files may be furnished.

Pantone Matching System will be used for color identification.

GPO Form 952 (Desktop Publishing – Disk Information) will be furnished.

Small package common carrier instructions and account number.

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

EXHIBITS:

Exhibit A - Contractor Personnel Security Certification, SSA-301

Exhibit B - Controlled Unclassified Information – System Security Plan (CUI-SSP) Template

Exhibit C - NIST Special Publication 800-53 SSP

Exhibit D - NIST Special Publication 800-171 SSP

Exhibit E -SSA PII Loss Reporting Template

Exhibit F: General Records Schedule 4.2, Information Access and Protection Records, Item 40

Exhibit G: Form SSA-222

Exhibit H - Sample Stock Replenishment Task Order*

Exhibit I - Sample Fulfillment Task Order*

Exhibit J - Initial Stock Retrieval Report*

Exhibit K - Daily Inventory Update File Template*

Exhibit L - Daily Replenishment Status Update File Template*

Exhibit M - Daily Fulfillment Status Update File Template*

Exhibit N - Printed Items Specification data table*

Exhibit O - Initial Stock Retrieval Report*

Exhibit P - Packing Slip Template

Exhibit Q - Yellow Label for Customer Random Copies

* These exhibits were originally in MS Excel and are available in that format upon request.

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

Contractor is required to set up, establish, and maintain a contractor-hosted SFTP website that multiple users at SSA can access. The SFTP website must be accessible via Edge web browser and must not require the download or installation of any additional software.

The contractor's SFTP site must be available 24 hours a day, seven (7) days a week.

NOTE: Contractor cannot send any notices of information that contain PII via email. Appropriate log-on instructions and protocol must be provided by the contractor at time of award. The contractor shall provide security, which at a minimum, shall require a unique user ID and password for each user to access.

PERFORMANCE TEST (Preproduction Test):

The purpose of this test is to determine if the end-to-end operations of the contractor's fulfillment workflow will meet the needs of SSA. This test will cover the receiving of SSA fulfillment stock and receiving and processing of a test fulfillment task order, processing of data, fulfillment of SSA customer orders (picking, packing, and staging for shipment) in the fulfillment task order, and response to SSA with Fulfillment Status Update and Inventory Update files.

The contractor will be required to pick up a predetermined portion of the initial inventory in order to perform the Work Performance Test. Once the pre-determined portion of the initial stock (as specified on the print order) is received and logged into inventory, the contractor will be required to demonstrate their ability to receive and generate data requirements from furnished data received via the contractor-hosted SFTP by completing a work performance test.

The contractor will be required to provide an inventory report prior to the work performance test to show inventory on hand prior to the test.

The contractor will be required to receive a test fulfillment task order file and prepare mock SSA customer orders (gathering and packing required items for fulfillment) from the file for shipping as described in these specifications as if they were in production mode. All elements of production are to be performed, including output of the Fulfillment Status Update File and Inventory Update File. The only exception of this test is that the contractor will not actually ship orders but will instead unpack and restock items once the test is complete.

At the end of the test, the contractor will provide SSA a Fulfillment Status Update file as well as an Inventory Report to show that all orders were completed, and the inventory levels had changed due to fulfillment. The contractor will then restock the test materials and apply the volumes back to their inventory.

Contractor must complete the test within three (3) workdays of receipt of furnished test fulfillment task order file. Once the contractor begins the fulfillment stage of the Work Performance Test they must complete all fulfillments, Status Update Reports, and Inventory Reports back to SSA withing one (1) workday.

NOTE: SSA will be on site for the test.

The Government will approve, conditionally approve, or disapprove the test the SAME day as the test occurs. Approval or conditional approval shall not relieve the contractor from complying with the specifications and all other terms and conditions of the contract. A conditional approval shall state any further action required by the contractor. A notice of disapproval shall state the reasons therefore.

If the test is disapproved by the Government, the Government, at its option, may require the contractor to perform an additional test, or just the failed portion of the test, in the time and under the terms and conditions specified in the notice of rejection. This additional test shall be at no additional cost to the Government. The Government will require the time specified above to inspect and test any additional samples required.

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

NOTE: If the contractor is defaulted, the contractor may be required to return all furnished materials/inventory to a location to be specified, at contractor's expense.

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

All costs, including the costs of the test, shall be included in the contract price for the production and fulfillment quantity. The test shall be performed at the facilities in which the contract production quantities are to be stocked and fulfillment processed.

Daily Update Files: The following update files must be provided daily (Monday through Friday) to SSA by 7:00 p.m., EST:

Daily Inventory Update Files (See Exhibit K) –

- The file format for Daily Inventory Updates must be Excel ".xls."
- The purpose of the Daily Inventory Updates is to provide information back to SSA on the current volume of each item stocked for fulfillment.
- Any item that is on back order must be reported as a negative value to show that backorders are being collected for later fulfillment.
- The Daily Inventory Update will follow a standard format (see Exhibit K).
- The contractor will be notified 20 workdays in advance of any file format changes.
- Example of Excel Format Name: "StatusUpdate_InventoryReport_YYYY-MM-DD.xls" (YYYY-MM-DD will be replaced with the actional date the file is being provided on.)
- These files will be transmitted to SSA via SFTP.

Daily Replenishment Status Update files (See Exhibit L) –

- The file format for Daily Replenishment Status Updates must be Excel ".xls."
- The purpose of the Daily Replenishment Status Update file is to provide information back to SSA on completed replenishment requests. For example, SSA submits a replenishment request via the replenishment task order. Contractor either prints or receives the stock into inventory. The following day's daily Replenishment Status Update file will contain the replenished items.
- The file will contain information on Replenishment items that were both printed and received the previous workday.
- The daily Replenishment Status Update files will follow a standard format (see Exhibit L).
- The contractor will be notified 20 workdays in advance of any file format changes.
- Example of Excel Format Name: "StatusUpdate_replenishment_YYYY-MM-DD.xls" (YYYY-MM-DD will be replaced with the actual date the file is being provided on.)
- These files will be transmitted to SSA via SFTP.

Daily Fulfillment Status Update files (See Exhibit M) –

- The file format for Daily Fulfillment Status Updates must be Excel ".xls."
- The purpose of the Daily Fulfillment Status Update file is to provide information back to SSA on the previous day's fulfillments.
- The file will contain information on fulfillment items that were fulfilled, placed on back order, and cancelled the previous workday.
- The Daily Fulfillment Status Update files will follow a standard format (see Exhibit M).
- The contractor will be notified 20 workdays in advance of any file format changes.
- Example of Excel Format Name: "StatusUpdate_Fulfillment_YYYY-MM-DD.xls" (YYYY-MM-DD will be replaced with the actual date the file is being provided on.)
- These files will be transmitted to SSA via SFTP.

CONTRACT START-UP AND TRANSFER OF INVENTORY:

Contractor will be responsible for the pickup of materials to be placed in the contractor's inventory for fulfillment of orders. (See "GOVERNMENT TO FURNISH, *Furnished Inventory*.")

Immediately after award, the contractor must contact the ordering agency to make arrangements for the transfer of materials from a warehouse location within a 250-mile radius of SSA's Headquarters (Baltimore, MD), to the contractor's facility. The contractor will be reimbursed for all shipping costs by submitting all shipping receipts with the billing invoice.

ELECTRONIC PREPRESS (Orders Produced by Contractor): Prior to image processing, the contractor shall perform a basic check (preflight) of the furnished media and publishing files to assure correct output of the required reproduction image. The preflight must identify any problem areas with digital file submission, to include but not is not limited to, missing or damaged fonts, damaged discs, missing bleeds, improper trim size, and/or improper color definition. Any errors, media damage, or data corruption that might interfere with proper file image processing must be reported to: Matthew Thomas at matthew.thomas@ssa.gov.

The contractor shall create or alter any necessary trapping, set proper screen angles and screen frequency, and define file output selection for the imaging device being utilized. Furnished files must be imaged as necessary to meet the assigned quality level.

All halftones are to be 150-line screen or finer.

PROOFS: SSA uses many of the same publications and forms in several of its print contracts. To reduce the proofing requirements for any revisions, if it is determined after award that the awarded contractor is responsible for the production of any other SSA workloads containing the same publications and/or forms required for this program, then the revisions may be proofed using one of the other programs.

For Contractor Produced Products:

- When ordered, three (3) sets of digital color content proofs of the entire product. Direct to plate must be used to produce the final product with a minimum of 2400 x 2400 dpi. Proofs must be created using the same Raster Image Processor (RIP) that will be used to produce the product. Proofs shall be collated with all elements in proper position (not pasted up), imaged face and back, trimmed, and folded to the finished size of the product.
- When ordered, one (1) press quality PDF soft proof (for content only) using the same Raster Image Processor (RIP) that will be used to produce the final printed product. PDF proof will be evaluated for text flow, image position, and color breaks. Proof will not be used for color match.

Once SSA provides an "O.K. to Print" on the initial proofs for an item, that approved proof will be the standard for all orders requiring production of that particular item. Should new items be added, a proof of the new items will be required. Should any changes be made to an item (updated version, etc.), SSA will provide new copy, and a new proof will be required. (See "NEW AND UPDATED PRODUCTS.")

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

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

NEW AND UPDATED PRODUCTS: Throughout the life of the contract, SSA will update items and add new items to be produced by the contractor. Requests to update current items and addition of new items will be submitted to the contractor via email.

When the contractor is required to update an item, proofs will be required in accordance with the requirements as specified under "PROOFS." Updated proofing will be billed against the next available replenishment print order once the contractor receives the "O.K. to Print" from SSA.

If a product is updated and contains a disposition instruction to "Destroy Old Stock," then the contractor will remove and destroy all old edition dated material upon receipt of the "O.K. to Print" of the new edition. Upon destruction of the outdated stock, the contractor will report a zero (0) inventory of the item in the next day's inventory report. The contractor will begin back ordering the item until SSA issues a replenishment for the item.

If a product is updated and contains a disposition instruction to "Use Prior Edition," then the contractor will use up the current edition of the materials. Once a replenishment for the item is requested, the contractor will only print the newest edition of the material.

STOCK/PAPER: The specifications of all paper furnished must be in accordance with those listed herein or listed for the corresponding JCP Code numbers in the "Government Paper Specification Standards No. 13" dated September 2019.

Government Paper Specification Standards No. 13 –
https://www.gpo.gov/docs/default-source/forms-and-standards-files-for-vendors/vol_13.pdf.

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

All text paper used in each copy must be of a uniform shade. Color of paper must remain consistent between different print runs throughout the term of the contract. All cover paper must have the grain parallel to the spine.

The paper to be used for each printed product will be indicated on the furnished specification spreadsheet provided (see Exhibit N). As items are added, a revised specification spreadsheet will be provided.

Cut Sheet Forms (Formats A through C):

White Writing, basis weight: 16 lbs. per 500 sheets, 17 x 22", equal to JCP Code D10.

White Writing, basis weight: 20 lbs. per 500 sheets, 17 x 22", equal to JCP Code D10; or, at contractor's option, White Uncoated Text, basis weight: 50 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60.

Colored Writing (Blue, Buff, Green, Pink, Salmon, and Yellow), basis weight: 20 lbs. per 500 sheets, 17 x 22", equal to JCP Code D10.

White Ledger, basis weight: 44 lbs. per 500 sheets, 17 x 22", equal to JCP Code J10; or, at contractor's option, White Index, basis weight: 90 lbs. per 500 sheets, 25-1/2 x 30-1/2", equal to JCP Code K10.

Booklet Forms (Format D):

White Writing, basis weight: 20 lbs. per 500 sheets, 17 x 22", equal to JCP Code D10; or, at contractor's option, White Uncoated Text, basis weight: 50 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60.

Colored Writing (Blue, Buff, Green, Pink, Salmon, and Yellow), basis weight: 20 lbs. per 500 sheets, 17 x 22", equal to JCP Code D10; or, at contractor's option, Uncoated Colored Text, basis weight: 50 lbs. per 500 sheets, 25 x 38", equal to JCP Code A63.

*Fact Sheet Publications (Format E)***:**

White Uncoated Text, basis weight: 60 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60.

Leaflet Publications (Formats F through K):

White Uncoated Text, basis weight: 60 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60.

Booklet Publications (Formats L and M):

White Uncoated Text, basis weight: 60 lbs. per 500 sheets, 25 x 38", equal to JCP Code A60.

PRINTING:

Match Pantone number as indicated on the furnished GPO Form 952.

Cut Sheet Forms (Formats A through C): Print face only or face and back, head-to-head or head-to-side, in one ink color. Some forms may contain a screen tint.

Booklet Forms (Format D): Print head-to-head, head-to-foot, or head-to-side, as required, in a single ink color.

Fact Sheet Publications (Format E): Print face only or face and back, head-to-head in two ink colors.

Leaflet Publications (Formats F through K): Print face and back in two ink colors. Contractor may be required to create a graduation of a two-color blend on the front panel only. Leaflets may contain halftones.

Booklet Publications (Formats L and M): Print head-to-head in two ink colors. Bleed pages scattered throughout.

PRESS SHEET INSPECTION: Final makeready press sheets may be inspected and approved at the contractor's plant for the purpose of establishing specified standards for use during the actual press run. Upon approval of the sheets, contractor is charged with maintaining those standards throughout the press run (within QATAP tolerances when applicable) and with discarding all makeready sheets that preceded approval. When a press sheet inspection is required, it will be specified on the individual print order. See GPO Publication 315.3 (Guidelines for Contractors Holding Press Sheet Inspections) issued January 2015.

NOTE: A press sheet inspection is for the purpose of setting specific standards that are to be maintained throughout the entire run. It does not constitute a prior approval of the entire run.

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

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

MARGINS: Unless otherwise specified, margins will be as indicated on the furnished GPO Form 952 or specified for each form product.

BINDING AND CONSTRUCTION: Various binding and construction styles will be ordered as follows:

Cut Sheet Forms (Formats A through C): Trim four sides.

Booklet Forms (Format D): Paste on fold and trim three sides or saddle-wire stitch in two places and trim three sides. Each product must contain complete four-page signatures after trimming. Single leaves connected with a lip (i.e., binding stub) to left of right of stitches will not be allowed.

Fact Sheet Publications (Format E): Trim four sides.

Leaflet Publications (Format F through K): Fold from flat size 7 x 8", 10-1/2 x 8", 14 x 8", 17-1/2 x 8", 21 x 8", or 24-1/2 x 8" (as ordered) down to 3-1/2 x 8" with up to six (6) wraparound folds, title out.

Booklet Publications (Formats L and M): Saddle-wire stitch in two places and trim three sides. Each product must contain complete four-page signatures after trimming. Single leave connected with a lip (i.e., binding stub) to left or right side of stitches is not allowed.

Perforating/Scoring: One or more perforations/scores, as ordered, may be required on approximately 40 percent of all cut sheet forms, and booklet forms, that are ordered.

Drilling: Drill two round holes, 1/4" or 9/32" in diameter, at the top, left, and/or right, through some or all parts as indicated. Holes are to be 2-3/4" center to center. Center of holes to be 3/8" from top edge of form on the top dimension (centered); or 3/8" in from left or right side of the product and centered.

PRODUCTION INSPECTION: Production inspection(s) may be required at the contractor's plant for the purpose of establishing that the receipt of transmitted files, the gathering of product items, inserting, and shipping/mailing is being accomplished in accordance with contract quality attributes, requirements, and 100% accountability.

NOTE: A production inspection is for the purpose of setting specific standards that are to be maintained throughout the duration of the contract. When production inspection is required, the Government will notify the contractor.

PACKING: Contractor will be required to pack furnished inventory items in a variety of ways. SSA will identify the packing of each item in the Initial Stock Retrieval Report (Exhibit O) as well as in the replenishment task orders.

Shrink-film wrap the specified quantity of each contractor-produced item as specified in the specification spreadsheet.

Furnished mounted posters are to be packed flat in appropriately sized containers. Furnished un-mounted posters are to be packed flat in appropriately sized containers or rolled and inserted into tubes, at contractor's option.

It is the contractor's responsibility to assure that the correct package material is inserted into each kraft envelope, shipping bag, shipping bundle, and shipping container.

All shipments which fill less than a shipping container must be packaged with materials of sufficient strength and durability and in such a manner, which will guarantee that the product will not be damaged, and the package will not open nor split when processed through the U.S. mail system or small package carrier delivery system.

Gather the items for a specific order and pack as applicable below:

Single and multiple copies up to 200 total leaves (for all products) must be inserted into kraft envelopes.

Quantities over 200 leaves, up to 12 pounds, must be inserted into cushioned shipping bags or wrapped in shipping bundles (maximum gross weight 14 pounds).

Quantities over 12 pounds, up to 36 pounds, must be packed in shipping containers (maximum gross weight 40 pounds).

Contractor must insert a packing slip for each order listing the contents of the shipment and any items that may be out of stock at the time of initial fulfillment. (See Exhibit P)

LABELING AND MARKING: It is the contractor's responsibility to assure the correct label is affixed to each shipment. An occasional order may require the outputting of multiple address labels to a single destination.

Create and affix a recipient address label to each unit of mail packaged in kraft envelopes, shipping bags, shipping bundles, and shipping containers. At contractor's option, addresses may be imaged directly onto the kraft envelopes, shipping bags, shipping bundles, and shipping containers.

CUSTOMER RANDOM COPIES (YELLOW LABEL): All replenishment requests must be divided into equal sublots in accordance with the chart below. A random copy must be selected from each sublot. Do not choose copies from the same general area in each sublot.

The contractor will be required to execute a statement furnished by the agency certifying that copies were selected as directed. The random copies constitute a part of the total quantity ordered, and no additional charge will be allowed.

Quantity Ordered	Number of Sublots
100 – 3,200	5
3,200 – 10,000	10
10,000 – 35,000	15
35,000 and over	20

These randomly selected copies must be packed separately and identified by a special Government-furnished YELLOW LABEL, affixed to each affected container. The container and its contents shall be recorded separately on all shipping documents and sent in accordance with the distribution list to the address indicated.

The Replenishment Task Order Number and a signed Government-furnished certificate of selection must be included. (See Exhibit Q for Certificate of Selection for Yellow Labels.)

Yellow labels will be shipped to the attention of the SSA analyst listed on the "Stock Replenishment Task Order File" (see Exhibit H) in the "Submitted By" column for each respective replenishment request.

All yellow label samples will be shipped to: SSA, Attn: "Submitted By," 1300 Annex Building, 6401 Security Boulevard, Baltimore, MD 21235.

DEPARTMENTAL RANDOM COPIES (BLUE LABEL): (Replenishment Requests on Task Orders Only): All requests must be divided into equal sublots in accordance with the chart below. A random copy must be selected from each sublot. Do not choose copies from the same general area in each sublot. The contractor will be required to certify that the copies were selected as directed using GPO Form 917 – Certificate of Selection of Random Copies (located on www.GPO.gov). The random copies constitute a part of the total quantity ordered, and no additional charge will be allowed.

Quantity Ordered	Number of Sublots *
500 - 3,200	50
3,201 - 10,000	80
10,001 - 35,000	125
35,001 and over	200

*** NOTE**: The number of sublots noted above are the minimum required. If additional quantities need to be included due to packaging requirements, that is acceptable.

These randomly selected copies must be packed separately and identified by a special label, GPO Form 2678 – Departmental Random Copies (Blue Label). This form, which can be downloaded from www.GPO.gov, must be printed on blue paper and affixed to each affected container or shrink packed unit to make them easily identifiable. A copy of the Replenishment Task Order/specification and a signed Certificate of Selection of Random Copies must be included and remain with the copies stored by the contractor. The contractor will stock these samples with the ordered quantity. These copies are to be used last for fulfillment and distribution. At any time during the ordered quantities life in inventory, SSA or GPO may request these samples to review for quality.

A copy of the signed Certificate of Selection of Random Copies must accompany the invoice sent to U.S. Government Publishing Office, Financial Management Services, for payment. Failure to furnish the certificate may result in delay in processing the invoice.

QUALITY ASSURANCE RANDOM COPIES: In addition to the Departmental Random Copies (Blue Label), the contractor may be required to submit quality assurance random copies to test for compliance against the specifications. The print order will indicate the number required, if any. When ordered, the contractor must divide the entire order into equal sublots and select a copy from a different general area of each sublot.

The contractor will be required to certify that the copies were selected as directed using GPO Form 917 – Certificate of Selection of Random Copies which can be located on www.GPO.gov. Copies will be paid for at the running rate offered in the contractor's bid, and their cost will not be a consideration for award. A copy of the print order must be included with the samples.

Business Reply Mail labels will be furnished for mailing the quality assurance random copies. The copies are to be mailed at the same time as the first scheduled shipment. A U.S. Postal Service approved Certificate of Mailing, identified by GPO program, jacket, and print order numbers must be furnished with billing as evidence of mailing.

DISTRIBUTION (Fulfillment Orders): Mail/ship f.o.b. contractor's city to addresses nationwide, including Alaska, Hawaii, and the American Territories and Possessions.

The contractor will be required to mail/ship via USPS Priority Mail or Small Package Common Carrier (SPCC) via 3rd Party or Prepaid Billing to as many as 1,400 destinations. SSA will determine the SPCC billing option (3rd Party or Prepaid) and provide instructions after award.

Shipments to the 48 Contiguous States, Alaska, Hawaii, and Puerto Rico are to be shipped using SSA provided Small package Common Carrier (SPCC).

Shipments to U.S. Territories and Possessions of American Samoa, Federated States of Micronesia, Guam, Marshall Islands, Northern Mariana Islands, Palau, U.S. Virgin Islands, Wake Island, and USPS P.O. Boxes must be made by reimbursable U.S. Postal Service First Class/Priority Mail. The contractor will be reimbursed for all U.S. Postal Service shipping costs by submitting all shipping receipts with the invoice for billing.

USPS Priority Mail:

The contractor is responsible for all costs incurred in transporting this product to the post office.

Reimbursable USPS Priority Mail will be used when shipping to the aforementioned U.S. Territories and Possessions. The contractor will be required to mail to the aforementioned U.S. Territories and Possessions via USPS Priority Mail rates.

The contractor is required to prepare mail in accordance with appropriate USPS rules and regulations, including the USPS domestic Mail Manual (DMM), Postal bulletins, and other USPS rules and regulations in effect at the time of mailing.

Mail pieces addressed to these U.S. Territories and Possessions will mail by USPS "Priority Mail." The contractor may use "free of charge" USPS "Priority" flat rate mail envelopes, bags, bundles, and containers (as allowed for Priority Mail). Contractor is responsible for ensuring adequate supplies of these envelopes/containers are available at all times. Contractor must use these flat rate envelopes/containers appropriately (fill to capacity).

Contractor will be reimbursed for all Priority Mailing costs upon receipt of all mailing receipts with their billing invoice.

Small Package Common Carrier (SPCC):

Packages weighing over 13 ounces and up to and including 499 pounds are to be made by SPCC (NO mailing via USPS) except those destined for Post Office Boxes, APO/FPO addresses, and U.S. Possessions and Territories as specified above.

The Social Security Administration will provide the name of the small package common carrier. When the service of a small package common carrier is used, the contractor will be responsible for providing the carrier with the following:

1. All packages are addressed and sorted to meet the requirements of the small package common carrier.

   NOTE: Contractor may be required to apply special SPCC barcode labels.

2. Separate common carrier pickup record(s) for each print order. The contractor must annotate the pickup record(s) with the requisition number and the print order number.

3. A shipping manifest which includes:

   a) Name of contractor, the requisition number, the task order number, and the common carrier account/shipper number.

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

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

   d) Summary information for each group, including total number of packages, total weight, and total shipping cost.

Within seven (7) workdays of completion of all task order requirements of the print order, contractor must email a PDF copy of their billing invoice to: Matthew.Thomas@ssa.gov.

Upon completion of the contract, contractor must return furnished any physically provided Government furnished materials to: SSA, Attn: Matthew Thomas, 1300 Annex Building, Baltimore, MD 21235.

All expenses incidental to picking up and returning materials (when applicable), submitting proofs, and furnishing sample copies must be borne by the contractor.

SCHEDULE: Adherence to this schedule must be maintained. Contractor must not start production of any job prior to receipt of the individual print order (GPO Form 2511) or task order, as applicable.

Task orders will be furnished via contractor-hosted SFTP. Print orders will be furnished via email.

Furnished material (when applicable) and hard copy proofs must be picked up from and delivered to: SSA, Attn: Matthew Thomas, 1300 Annex Building, Baltimore, MD 21235.

When applicable, furnished electronic media and visuals must be returned with hard copy proofs.

When required, PDF proofs will be transferred to the agency via a contractor-provided secure site or email, as specified. Contractor to follow up with phone call confirming receipt. If emailing, the subject line of the email must include the Product ID number and "PROOF."

Proofing Schedule

Initial Product Proofing Schedule:

The following schedule begins the workday after receipt of the furnished materials. The workday after receipt will be the first workday of the schedule.

- The contractor will submit PDF soft proofs for all products within 10 workdays of receipt of furnished materials.
- Proofs will be withheld no more than 10 workdays from their receipt at the ordering agency until changes/corrections/"O.K. to Print" are furnished to the contractor (either by SFTP or email).

  NOTE: The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.

- If required due to AA's, the contractor must submit revised proofs within five (5) workdays of receipt of marked-up proofs. (No additional time will be allowed due to printer's errors (PE's).)

- Revised proofs will be withheld no more than five (5) workdays from their receipt at the ordering agency until changes/corrections/"O.K. to Print" are furnished to the contractor (either by SFTP or email).

  NOTE: The first workday after receipt of revised proofs at the ordering agency is day one (1) of the hold time.

- The contractor will keep the furnished material on file for each item that receives an "O.K. to Print" to produce future replenishments.

***Proofing Schedule for New and Updated Items (Contractor-Produced)*:**

Throughout the life of the contract, SSA will either update existing items or add new items. The contractor will receive requests for updated and new materials via email and/or SFTP. The following schedule begins the workday after receipt of the request. The workday after receipt will be the first workday of the schedule.

- The contractor will submit PDF soft proofs for updated and new items within three (3) workdays of receipt of update request and furnished materials.
- Proofs will be withheld no more than three (3) workdays from their receipt at the ordering agency until changes/corrections/"O.K. to Print" are furnished to the contractor (either by SFTP or email). The first workday after receipt of proofs at the ordering agency is day one (1) of the hold time.
- If required due to AA's, the contractor must submit revised proofs within three (3) workdays of receipt of marked-up proofs. (No additional time will be allowed due to printer's errors (PE's).)
- Revised proofs will be withheld no more than three (3) workdays from their receipt at the ordering agency until changes/corrections/"O.K. to Print" are furnished to the contractor (either by SFTP or email). The first workday after receipt of revised proofs at the ordering agency is day one (1) of the hold time.
- The contractor will keep the most current furnished materials on file for each item that receives an "O.K. to Print" to fulfill future replenishments.

Production Schedule

The schedule will begin the workday after receipt of a replenishment task order. The workday after receipt will be the first workday of the schedule.

***Replenishment Schedule**:* The contractor will have 15 workdays to complete the production of each replenishment as follows:

- Complete production of the required products.
- Label each unit of issue with an inventory label.
- Stock the items for fulfillment.
- Notify SSA of the item's status via the Replenishment Status Update File.

Receiving Schedule:

The contractor will have two (2) workdays after an item is received to complete the following tasks. The workday after receipt of an item will be the first workday of the schedule.

- Inspect the quality of the received items and report any damages back to SSA.
- Label each unit of issue with an inventory label.
- Stock the items for fulfillment.
- Notify SSA of the item's status via the Replenishment Status Update File.

Fulfillment and Distribution Schedule:

The following schedule begins the SAME workday as receipt of fulfillment task order file; the same workday as receipt will be the first workday of the schedule.

- Fulfillment task order files will be transmitted on a daily basis, Monday through Friday.
- The contractor must complete fulfillment and distribution within three (3) workdays of receipt of each fulfillment task order.
    - Each order shipment will include a packing slip specifying what is included in the order shipment. Any item that is out of stock at the time of initial fulfillment will be listed on the packing slip as "Backorder."
    - If an item is out of stock, the contractor must include the item in their Daily Fulfillment Status Update files as on Backorder (indicated as "B" for Status - See Exhibit M). Reporting an out of stock item as Backorder within the three (3) workday period will constitute as timely.

Press Sheet or Production Inspection:

The contractor must notify the GPO and SSA of the date and time the Press Sheet Inspection and/or Production Inspection can be performed. In order for proper arrangements to be made, notification must be given at least three (3) workdays prior to the inspection.

Notify the U.S. Government Publishing Office, Quality Control for Published Products, Washington, DC 20401 at (202) 512-1162 or (202) 512-0542 AND Matthew Thomas with SSA via email at (matthew.thomas@ssa.gov). Telephone calls will only be accepted between the hours of 8:00 a.m. and 2:00 p.m., prevailing Eastern Time, Monday through Friday.

NOTE: See contract clauses, paragraph 14(e)(1), Inspections and Tests of GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987 (Rev. 01-18)).

When supplies are not ready at the time specified by the contractor for inspection, the Contracting Officer may charge to the contractor the additional cost of the inspection.

The ship/deliver date indicated on the print order is the date ordered for mailing/shipping f.o.b. contractor's city must be delivered to the U.S. Postal Service or picked up by small package common carrier.

Unscheduled material such as shipping documents, receipts or instructions, delivery lists, labels, etc., will be furnished with each order or shortly thereafter. In the event such information is not received in due time, the contractor will not be relieved of any responsibility in meeting the shipping schedule because of failure to request such information.

For compliance reporting purposes, the contractor is to notify the U.S. Government Publishing Office of the date of shipment or delivery. Upon completion of each order, contractor must contact the Shared Support Services Compliance Section via email at compliance@gpo.gov, or via telephone at (202) 512-0520. Personnel receiving the email or call will be unable to respond to questions of a technical nature or to transfer any inquiries.

DAILY FULFILLMENT STATUS UPDATE FILES: A fulfillment status update file will be created by the contractor at the end of each workday summarizing what was packaged and shipped, put on back order, or cancelled.

The report will be transmitted to SSA via SFTP Monday through Friday. If the contractor elects to fulfill orders on Saturday and Sunday, then those updates will be included on Monday evening's fulfillment status update file.

DAILY REPLENISHMENT STATUS UPDATE FILES: A replenishment status update file will be created by the contractor at the end of each workday summarizing what was printed and stocked, or received and stocked for fulfillment. The report will be transmitted to SSA via SFTP Monday through Friday. If the contractor elects to replenish items on Saturday and Sunday, then those updates will be included on Monday evening's fulfillment status update file.

DAILY INVENTORY REPORTS: An inventory update file will be created by the contractor at the end of the workday summarizing what the current inventory of each item on hand is. The Inventory Report will be created and sent at the same time each day.

STORAGE AND MAINTENANCE OF INVENTORY: The title(s) of Government-furnished materials shall remain in the Government. The contractor shall maintain adequate property control records of all Government-furnished materials in accordance with industrial practices.

The contractor will be required to store items in a manner that provides protection from any type of damage from the elements.

The Government anticipates that approximately 53,000 cubic feet of space will be needed for the storage of inventory for: 1) start-up inventory furnished by SSA at the beginning of the contract; 2) inventory furnished by SSA throughout the term of the contract; and, 3) products produced by the contractor that go into inventory for later fulfillment.

Unless otherwise provided in this contract, the contractor, upon receipt and acceptance of any Government-furnished material, assumes the risk of, and shall be responsible for loss thereof, or damage thereto, except to the extent that such material is consumed in the performance of this contract.

The contractor will be responsible for counting/verifying products furnished for start-up inventory and anytime throughout the term of the contract. Contractor must notify the Government of any shortage within 24 hours of receipt thereof.

Controlled Storage Area: Temperature and humidity-controlled storage area is required for sensitive fulfillment items. Items requiring controlled storage will be received items and not printed items. Sensitive items requiring controlled storage will be flagged in the Initial Stock Retrieval Report (Exhibit J). An example of items requiring controlled storage are envelopes and decals. Storage location must maintain a threshold of 30 to 50% humidity and 65 to 75 degrees Fahrenheit.

ON-SITE INSPECTION OF STORAGE FACILITY: On a quarterly basis, the ordering agency will conduct an on-site inspection of the contractor's storage facility to ensure that the products (both contractor-produced and Government-furnished) are being stored and fulfilled in accordance with these specifications.

At any point in the contract, the inspections may occur more frequently (bi-monthly or monthly).

The purpose of the inspections will be for SSA to check the inventory levels and edition dates of products. Additionally, SSA will inspect the quality of the products in inventory (both Government-furnished and contractor-produced).

The contractor will be notified 48 hours in advance of the inspection; however, SSA may have an unannounced on-site inspection.

SECTION 3. – DETERMINATION OF AWARD

The Government will determine the lowest bid by applying the prices offered in the "SCHEDULE OF PRICES" to the following units of production which are the estimated requirements to produce one (1) year's production under this contract. These units do not constitute, nor are they to be construed as, a guarantee of the volume of work which may be ordered for a like period of time.

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

		(1)	(2)	(3)
I.	(a)	262	12	10
	(b)	240		
	(c)	5		

II.		(1)	(2)
1.	(a)	4	12
	(b)	15	156
2.	(a)	1	7
	(b)	5	16
3.	(a)	10	2,889
4.	(a)	404	1,302
5.	(a)	23	306
	(b)	126	1,129
6.	(a)	6	974
7.	(a)	18	212
8.	(a)	25	336
9.	(a)	28	429
10.	(a)	6	42
11.	(a)	3	17
12.	(a)	660	22,228
13.	(a)	1,308	34,908

III.

1.	(a)	2
	(b)	67
	(c)	7
	(d)	93
2.	(a)	22
3.	(a)	2,889
4.	(a)	336
	(b)	316
5.	(a)	1,435
6.	(a)	974
7.	(a)	212
8.	(a)	336
9.	(a)	429
10.	(a)	42
11.	(a)	17
12.	(a)	11,114
13.	(a)	17,454

IV.	(a)	(1)	48
		(2)	3,102
	(b)		156
	(c)		150,380
	(d)		12
	(e)		16,754
	(f)		1

V.	(a)	4,918
	(b)	25,871
	(c)	26,945

SECTION 4. – SCHEDULE OF PRICES

Bids offered are f.o.b. contractor's city.

Prices must include the cost of all required materials and operations for each item listed in accordance with these specifications.

Bidder must make an entry in each of the spaces provided. Bids submitted with any obliteration, revision, or alteration of the order and manner of submitting bids may be declared non-responsive.

An entry of NC (No Charge) shall be entered if bidder intends to furnish individual items at no charge to the Government. Bids submitted with NB (No Bid), NA (Not Applicable), or blank spaces for an item may be declared non-responsive.

The Contracting Officer reserves the right to reject any offer that contains prices for individual items of production (whether or not such items are included in the DETERMINATION OF AWARD) that are inconsistent or unrealistic in regard to other prices in the same offer or to GPO prices for the same operation if such action would be in the best interest of the Government.

All invoices submitted to the GPO shall be based on the most economical method of production. Fractional parts of 1,000 will be prorated at the per-1,000 rate.

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

Formats D, L, and M: A charge will be allowed for each text page of a single-color product, whether printed or blank. Unless otherwise specified, no more than three blank pages may be permitted at the end of the text for saddle-stitched products.

Cost of all required paper must be charged under Item III. "PAPER."

I. PREPRESS OPERATIONS:

	Up to and including 8-1/2 x 11" (1)	Over 8-1/2 x 11" up to and including 17 x 11" (2)	Over 17 x 11" up to and including 25-1/2 x 11" (3)
(a) Digital color content proof..... per trim/page-size unit.....	$_____	$_____	$_____
(b) PDF Soft Proof (Any Size Product) .....per file.....			$_____
(c) System Timework.....per hour.....			$_____

Electronic prepress operations that cannot be properly classified under any other item will be charged as "System Timework." Any charge made under "System Timework" must be supported by a statement outlining in detail the operation for which payment is claimed. In case of dispute, the Contracting Officer reserves the right to be the final judge as to the operations and/or number of hours chargeable under Item I.(c).

_____
(Initials)

II. PRINTING AND BINDING: Prices offered shall include the cost of all required materials and operations (excluding paper) necessary for the printing and binding of the product listed in accordance with these specifications.

	Makeready and/or Setup (1)	Running Per 1,000 Copies (2)
1. Format A (5-1/2 x 8-1/2" up to and including 8-1/2 x 11"):		
(a) Cut Sheet Forms: Printing face only in one ink color, including binding ..... per cut sheet.....	$_____	$_____
(b) Cut Sheet Forms: Printing face and back in one ink color, including binding ..... per cut sheet.....	$_____	$_____
2. Format B (Over 8-1/2 x 11" up to and including 17 x 11"):		
(a) Cut Sheet Forms: Printing face only in one ink color, including binding ..... per cut sheet.....	$_____	$_____
(b) Cut Sheet Forms: Printing face and back in one ink color, including binding ..... per cut sheet.....	$_____	$_____
3. Format C (Over 17 x 11" up to and including 25-1/2 x 11"):		
(a) Cut Sheet Forms: Printing face and back in one ink color, including binding ..... per cut sheet.....	$_____	$_____
4. Format D (8-1/2 x 11"):		
(a) Booklet Forms: Printing in a single ink color, including binding.....per page.....	$_____	$_____
5. Format E (8-1/2 x 11"):		
(a) Fact Sheet Publications: Printing face only in two ink colors, including binding ..... per fact sheet.....	$_____	$_____
(b) Fact Sheet Publications: Printing face and back in two ink colors, including binding ..... per fact sheet.....	$_____	$_____
6. Format F (7 x 8" flat):		
(a) Leaflet Publications: Printing face and back in two ink colors, including binding ..... per leaflet.....	$_____	$_____

_____
(Initials)

	Makeready and/or Setup (1)	Running Per 1,000 Copies (2)
7. Format G (10-1/2 x 8" flat):		
(a) Leaflet Publications: Printing face and back in two ink colors, including binding ..... per leaflet.....	$_____	$_____
8. Format H (14 x 8" flat):		
(a) Leaflet Publications: Printing face and back in two ink colors, including binding ..... per leaflet.....	$_____	$_____
9. Format I (17-1/2 x 8" flat):		
(a) Leaflet Publications: Printing face and back in two ink colors, including binding ..... per leaflet.....	$_____	$_____
10. Format J (21 x 8" flat):		
(a) Leaflet Publications: Printing face and back in two ink colors, including binding ..... per leaflet.....	$_____	$_____
11. Format K (24-1/2 x 8" flat):		
(a) Leaflet Publications: Printing face and back in two ink colors, including binding ..... per leaflet.....	$_____	$_____
12. Format L (3-1/2 x 8"):		
(a) Booklet Publications: Printing in two ink colors, including binding ..... per page.....	$_____	$_____
13. Format M (5-1/4 x 8"):		
(a) Booklet Publications: Printing in two ink colors, including binding ..... per page.....	$_____	$_____

III. PAPER: Payment for all paper supplied by the contractor under the terms of these specifications, as ordered on the individual print order/task 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 makeready or running spoilage must be included in the prices offered.

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

Formats A through C (Cut Sheet Forms) - One basic charge will be allowed for each page-size leaf, as applicable to the format.

_____
(Initials)

Format D (Booklet Forms) - One basic charge will be allowed for each page-size leaf.

Format E (Fact Sheet Publications) - One basic charge will be allowed for each page-size leaf.

Formats F through K (Leaflet Publications) – One basic charge will be allowed for each page-size leaf (flat size), as applicable to the format.

Formats L and M (Booklet Publications) – One basic charge will be allowed for each page-size leaf, as applicable to the format.

Per 1,000 Leaves

1. Format A (5-1/2 x 8-1/2" up to and including 8-1/2 x 11" (flat)):
   (a) White Writing (16-lb.) ..... $_____
   (b) White Writing (20-lb.) ..... $_____
   (c) Colored Writing (20-lb.) ..... $_____
   (d) White Ledger (44-lb.); or, at contractor's option,
   White Index (90-lb.) ..... $_____
2. Format B (Over 8-1/2 x 11" up to and including 17 x 11" (flat)):
   (a) White Writing (20-lb.) ..... $_____
3 Format C (Over 17 x 11" up to and including 25-1/2 x 11" (flat)):
   (a) White Writing (20-lb.) ..... $_____
4. Format D (8-1/2 x 11"):
   (a) White Writing (20-lb.); or, at contractor's option,
   White Uncoated Text (50-lb.) ..... $_____
   (b) Colored Writing (20-lb.); or, at contractor's option,
   Uncoated Colored Text (50-lb.) ..... $_____
5. Format E (8-1/2 x 11"):
   (a) White Uncoated Text (60-lb.) ..... $_____
6. Format F (7 x 8" (flat):
   (a) White Uncoated Text (60-lb.) ..... $_____
7. Format G (10-1/2 x 8" (flat)):
   (a) White Uncoated Text (60-lb.) ..... $_____
8. Format H (14 x 8" (flat)):
   (a) White Uncoated Text (60-lb.) ..... $_____
9. Format I (17-1/2 x 8" (flat)):
   (a) White Uncoated Text (60-lb.) ..... $_____
10. Format J (21 x 8" (flat)):
   (a) White Uncoated Text (60-lb.) ..... $_____

_____
(Initials)

Per 1,000 Leaves

11. Format K (24-1/2 x 8" (flat)):
    (a) White Uncoated Text (60-lb.) ..... $_____

12. Format L (3-1/2 x 8"):
    (a) White Uncoated Text (60-lb.) ..... $_____

13. Format M (5-1/4 x 8-1/2"):
    (a) White Uncoated Text (60-lb.) ..... $_____

IV. ADDITIONAL OPERATIONS:

NOTE: Cost submitted for line item IV.(d) must include the cost for the labeling and stocking of items, both Government-furnished and contractor-produced.

(a) Perforating/Scoring:

(1) Makeready and/or Setup (each perforation or score): ..... per line ..... $_____

(2) Running (Maximum 3 lines per run) ..... per 1,000 leaves ..... $_____

(b) Drilling ..... per 1,000 leaves ..... $_____

(c) Shrink-wrapping ..... per package ..... $_____

(d) Storage of inventory ..... per month ..... $_____

(e) Picking items for fulfillment ..... per individual fulfillment order ..... $_____

(f) Destruction of sensitive material ..... per 1,000 pieces ..... $ _____

V. PACKING AND DISTRIBUTION: Prices offered must be all-inclusive, as applicable, and must include the cost of packing; all kraft envelopes, cushioned shipping bags, shipping bundles, and shipping containers; all necessary wrapping and packing materials; labeling and marking; and, complete distribution, in accordance with these specifications.

(a) Single or multiple copies in kraft envelope (up to 200 leaves) ..... per envelope ..... $_____

(b) Single or multiple copies over 200 leaves,
up to 12 pounds, in cushioned shipping bags,
or wrapped in shipping bundles
(maximum gross weight 14 pounds) ..... per bag or bundle ..... $_____

(c) Quantities over 12 pounds, up to 36 pounds,
packed in shipping containers
maximum gross weight 40 pounds) ..... per container ..... $_____

_____
(Initials)

LOCATION OF WAREHOUSE: All storage and fulfillment will be made from:

_____
(Street Address)

_____
(City – State – Zip Code)

_____
(Initials)

SHIPMENTS: Shipments will be made from: City _____ State _____.

The city(ies) indicated above will be used for evaluation of transportation charges when shipment f.o.b. contractor's city is specified. If no shipping point is indicated above, it will be deemed that the bidder has selected the city and state shown below in the address block, and the bid will be evaluated and the contract awarded on that basis. If shipment is not made from evaluation point, the contractor will be responsible for any additional shipping costs incurred.

DISCOUNTS: Discounts are offered for payment as follows: _____ Percent _____ Calendar Days. See Article 12 "Discounts" of Solicitations Provisions in GPO Contract Terms (Publication 310.2).

AMENDMENT(S): Bidder hereby acknowledges amendment(s) number(ed) _____.

BID ACCEPTANCE PERIOD: In compliance with the above, the undersigned agree, if this bid is accepted within_____ calendar days (***90 calendar days unless a different period is inserted by the bidder***) from the date for receipt of bids, to furnish the specified items at the price set opposite each item, delivered at the designated points(s), in exact accordance with specifications.

NOTE: *Failure to provide a 90-day bid acceptance period may result in expiration of the bid prior to award.*

BIDDER'S NAME AND SIGNATURE: Unless specific written exception is taken, the bidder, by signing and submitting a bid, agrees with and accepts responsibility for all certifications and representations as required by the solicitation and GPO Contract Terms – Publication 310.2. When responding by email, fill out and return one copy of all pages in "SECTION 4. – SCHEDULE OF PRICES," including initialing/signing where indicated. Valid electronic signatures will be accepted in accordance with the Uniform Electronic Transactions Act, §2. Electronic signatures must be verifiable of the person authorized by the company to sign bids. *Failure to sign the signature block below may result in the bid being declared non-responsive.*

Bidder _____
(Contractor's Name) (GPO Contractor's Code)

_____
(Street Address)

_____
(City – State – Zip Code)

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

_____
(Person to be Contacted) (Telephone Number)

_____
(Email) (Fax Number)

THIS SECTION FOR GPO USE ONLY

Certified by: _____ Date: _____ Contracting Officer: _____ Date: _____
(Initials) (Initials)

EXHIBIT A

CONTRACTOR PERSONNEL SECURITY CERTIFICATION

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

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

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

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

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

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

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

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

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

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

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

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

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

EXHIBIT B

1. SYSTEM IDENTIFICATION

1.1. System Name/Title: [State the name of the system. Spell out acronyms.]

1.1.1. System Categorization: Moderate Impact for Confidentiality

1.1.2. System Unique Identifier: [Insert the System Unique Identifier]

1.2. Responsible Organization:

Name:	
Address:	
Phone:	

1.2.1. Information Owner - Government point of contact responsible for providing and/or receiving Controlled Unclassified Information (CUI)**:**

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.2.1.1. System Owner (assignment of security responsibility)**:**

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.2.1.2. System Security Officer:

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.3. General Description/Purpose of System: What is the function/purpose of the system? **[Provide a short, high-level description of the function/purpose of the system.]**

1.3.1. Number of end users and privileged users: **[In the table below, provide the *approximate* number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, etc. Add rows to define different roles as needed.]**

Roles of Users and Number of Each Type:

Number of Users	Number of Administrators/ Privileged Users

1.4. General Description of Information: Controlled Unclassified Information (CUI) information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at https://www.archives.gov/cui/registry/category-list. [**Document the CUI information types processed, stored, or transmitted by the system below**].

2. SYSTEM ENVIRONMENT

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note**:** *this does not require depicting every workstation or desktop*, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram.
[Insert a system topology graphic. Provide a narrative consistent with the graphic that clearly lists and describes each system component.]

2.1. Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component. **[Insert the reference/URL or note that the hardware component inventory is attached.]**

2.2. List all software components installed on the system. **[Insert the reference/URL or note that the software component inventory is attached.]**

2.3. Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization? **[Yes/No - If no, explain:]**

3. REQUIREMENTS

(Note: The source of the requirements is NIST Special Publication 800-171, dated December 2016)

Provide a thorough description of how all of the security requirements are being implemented or planned to be implemented. The description for each security requirement contains: 1) the security requirement number and description; 2) how the security requirement is being implemented or planned to be implemented; and 3) any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the requirement is not applicable to the system, provide rationale.

3.1. Access Control

3.1.1. Account Management

a. Define the types of system accounts allowed and prohibited.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Create, enable, modify, disable, and remove system accounts in accordance with policy, procedures, prerequisites, and criteria.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Specify:

1. Authorized users of the system,
2. Group and role membership, and
3. Access authorizations (i.e., privileges) for each account.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Authorize access to the system based on:

1. A valid access authorization and
2. Intended system usage.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

e. Monitor the use of system accounts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

f. Disable system accounts when:

1. The accounts have expired,
2. The accounts have been inactive for [Assignment: organization-defined time period],
3. The accounts are no longer associated with a user or individual,
4. The accounts are in violation of organizational policy, or
5. Significant risks associated with individuals are discovered.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

g. Notify account managers and designated personnel or roles within:

1. [Assignment: organization-defined time period] when accounts are no longer required.

2. [Assignment: organization-defined time period] when users are terminated or transferred.
3. [Assignment: organization-defined time period] when system usage or the need-to-know changes for an individual.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

h. Require that users log out of the system after [Assignment: organization-defined time period] of expected inactivity or when [Assignment: organization-defined circumstances].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.2. Access Enforcement:

Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.3. Information Flow Enforcement

Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.4. Separation of Duties

a. Identify the duties of individuals requiring separation.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Define system access authorizations to support separation of duties of individuals to reduce the risk of malevolent activity without collusion.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.5. Least Privilege

a. Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Authorize access to [Assignment: organization-defined security functions] and [Assignment: organization-defined security-relevant information].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Review the privileges assigned to roles or classes of users [Assignment: organization-defined frequency] to validate the need for such privileges.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Reassign or remove privileges, as necessary.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.6. Least Privilege – Privileged Accounts

a. Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Require that users (or roles) with privileged accounts use non-privileged accounts when accessing non-security functions or non-security information.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.7. Least Privilege – Privileged Functions

a. Prevent non-privileged users from executing privileged functions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Log the execution of privileged functions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.8. Unsuccessful Logon Attempts

a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action] when the maximum number of unsuccessful attempts is exceeded.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.9. System Use Notification

Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting access to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.10. Device Lock

a. Prevent access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.11. Session Termination

Terminate a user session automatically after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.12. Remote Access

a. Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Authorize each type of remote system access prior to establishing such connections.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Route remote access to the system through authorized and managed access control points.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Authorize the remote execution of privileged commands and remote access to security-relevant information.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.13. Withdrawn

Incorporated into 03.01.12.

3.1.14. Withdrawn

Incorporated into 03.01.12.

3.1.15. Withdrawn

Incorporated into 03.01.12.

3.1.16. Wireless Access

a. Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Authorize each type of wireless access to the system prior to establishing such connections.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Disable, when not intended for use, wireless networking capabilities prior to issuance and deployment.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Protect wireless access to the system using authentication and encryption.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.17. Withdrawn
Incorporated into 03.01.16.

3.1.18. Access Control for Mobile Devices

a. Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Authorize the connection of mobile devices to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Implement full-device or container-based encryption to protect the confidentiality of CUI on mobile devices.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.19. Withdrawn
Incorporated into 03.01.18.

3.1.20. Use of External Systems

a. Prohibit the use of external systems unless the systems are specifically authorized.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after:

1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and

2. Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.1.21. Withdrawn

Incorporated into 03.01.20.

3.1.22. Publicly Accessible Content

a. Train authorized individuals to ensure that publicly accessible information does not contain CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review the content on publicly accessible systems for CUI and remove such information, if discovered.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.2. Awareness and Training

3.2.1. Literacy Training and Awareness

a. Provide security literacy training to system users:
   1. As part of initial training for new users and [Assignment: organization- defined frequency] thereafter,
   2. When required by system changes or following [Assignment: organization- defined events], and
   3. On recognizing and reporting indicators of insider threat, social engineering, and social mining.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.2.2. Role-Based Training

a. Provide role-based security training to organizational personnel:
   1. Before authorizing access to the system or CUI, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter.
   2. When required by system changes or following [Assignment: organization-defined events].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.2.3. Withdrawn

Incorporated into 03.02 01.

3.3. Audit and Accountability

3.3.1. Event Logging

a. Specify the following event types selected for logging within the system: [Assignment: organization-defined event types].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update the event types selected for logging [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.2. Audit Record Content

a. Include the following content in audit records:
   1. What type of event occurred
   2. When the event occurred
   3. Where the event occurred
   4. Source of the event

5. Outcome of the event
6. Identity of the individuals, subjects, objects, or entities associated with the event.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Provide additional information for audit records as needed.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.3. Audit Record Generation

a. Generate audit records for the selected event types and audit record content specified in **03.03.01** and **03.03.02**.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Retain audit records for a time period consistent with the records retention policy.Review and update logged events.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.4. Response to Audit Logging Process Failures

a. Alert organizational personnel or roles within [Assignment: organization-defined time period] in the event of an audit logging process failure.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Take the following additional actions: [Assignment: organization-defined additional actions].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.5. Audit Record Review, Analysis, and Reporting

a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications and the potential impact of inappropriate or unusual activity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Report findings to organizational personnel or roles.
Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.6. Audit Record Reduction and Report Generation

a. Implement an audit record reduction and report generation capability that supports audit record review, analysis, reporting requirements, and after-the-fact investigations of incidents.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Preserve the original content and time ordering of audit records.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.7. Time Stamps

a. Use internal system clocks to generate time stamps for audit records.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.8. Protection of Audit Information

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Authorize access to management of audit logging functionality to only a subset of privileged users or roles.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3.9. Withdrawn

Incorporated into 03.03.08.

3.4. Configuration Management

3.4.1. Baseline Configuration

a. Develop and maintain under configuration control, a current baseline configuration of the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update the baseline configuration of the system [Assignment: organization-defined frequency] and when system components are installed or modified.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.2. Configuration Settings

a. Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Identify, document, and approve any deviations from established configuration settings.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.3. Configuration Change Control

a. Define the types of changes to the system that are configuration controlled.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security impacts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Implement and document approved configuration-controlled changes to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Monitor and review activities associated with configuration-controlled changes to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.4. Impact Analyses

a. Analyze changes to the system to determine potential security impacts prior to change implementation.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Verify that the security requirements for the system continue to be satisfied after the system changes have been implemented.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.5. Access Restrictions for Change

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.6. Least Functionality

a. Configure the system to provide only mission-essential capabilities.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Prohibit or restrict use of the following functions, ports, protocols, connections, and services: [Assignment: organization-defined functions, ports, protocols, connections, and services].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Review the system [Assignment: organization-defined frequency] to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.7. Withdrawn

Incorporated into 03.04.06 and 03.04.08.

3.4.8. Authorized Software – Allow by Exception

a. Identify software programs authorized to execute on the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Implement a deny-all, allow-by-exception policy for the execution of authorized software programs on the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Review and update the list of authorized software programs [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.9. Withdrawn

Addressed by 03.01.05, 03.01.06, 03.01.07, 03.04.08, and 03.12.03.

3.4.10. System Component Inventory

a. Develop and document an inventory of system components.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update the system component inventory [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Update the system component inventory as part of installations, removals, and system updates.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.11. Information Location

a. Identify and document the location of CUI and the system components on which the information is processed and stored.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Document changes to the system or system component location where CUI is processed and stored.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.4.12. System and Component Configuration for High-Risk Areas

a. Issue systems or system components with the following configurations to individuals traveling to high-risk locations: [Assignment: organization-defined system configurations].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Apply the following security requirements to the systems or components when the individuals return from travel: [Assignment: organization-defined security requirements].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5. Identification and Authentication

3.5.1. User Identification, Authentication, and Re-Authentication.

a. Uniquely identify and authenticate system users and associate that unique identification with processes acting on behalf of those users.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Re-authenticate users when [Assignment: organization-defined circumstances or situations requiring re-authentication].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.2. Device Identification and Authentication
Uniquely identify and authenticate [Assignment: organization-defined devices or types of devices] before establishing a system connection.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.3. Multi-Factor Authentication
Implement multi-factor authentication for access to privileged and non-privileged accounts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.4. Replay-Resistant Authentication
Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.5. Identifier Management

a. Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Select and assign an identifier that identifies an individual, group, role, service, or device.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Prevent the reuse of identifiers for [Assignment: organization-defined time period].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.6. Withdrawn

Consistency with SP 800-53.

3.5.7. Password Management

a. Maintain a list of commonly used, expected, or compromised passwords, and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Transmit passwords only over cryptographically protected channels.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Store passwords in a cryptographically protected form.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

e. Select a new password upon first use after account recovery.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

f. Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.8. Withdrawn
Consistency with SP 800-53.

3.5.9. Withdrawn
Consistency with SP 800-53.

3.5.10. Withdrawn
Incorporated into 03.05.07.

3.5.11. Authentication Feedback
Obscure feedback of authentication information during the authentication process.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.5.12. Authenticator Management
a. Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Establish initial authenticator content for any authenticators issued by the organization.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Change default authenticators at first use.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

f. Protect authenticator content from unauthorized disclosure and modification.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6. Incident Response

3.6.1. Incident Handling

Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6.2. Incident Monitoring, Reporting, and Response Assistance

a. Track and document system security incidents.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Report incident information to [Assignment: organization-defined authorities].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Provide an incident response support resource that offers advice and assistance to system users on handling and reporting incidents.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6.3. Incident Response Testing

Test the effectiveness of the incident response capability [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6.4. Incident Response Training

a. Provide incident response training to system users consistent with assigned roles and responsibilities:
   1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access,
   2. When required by system changes, and
   3. [Assignment: organization-defined frequency] thereafter.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.6.5. Incident Response Plan

a. Develop an incident response plan that:
   1. Provides the organization with a roadmap for implementing its incident response capability,
   2. Describes the structure and organization of the incident response capability,
   3. Provides a high-level approach for how the incident response capability fits into the overall organization,
   4. Defines reportable incidents,
   5. Addresses the sharing of incident information, and
   6. Designates responsibilities to organizational entities, personnel, or roles.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Distribute copies of the incident response plan to designated incident response personnel (identified by name and/or by role) and organizational elements.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Protect the incident response plan from unauthorized disclosure.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7. Maintenance

3.7.1. Withdrawn

Recategorized as NCO.

3.7.2. Withdrawn

Incorporated into 03.07.04 and 03.07.06.

3.7.3. Withdrawn

Incorporated into 03.08.03.

3.7.4. Maintenance Tools

a. Approve, control, and monitor the use of system maintenance tools.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Check media with diagnostic and test programs for malicious code before it is used in the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Prevent the removal of system maintenance equipment containing CUI by verifying that there is no CUI on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.5. Nonlocal Maintenance

a. Approve and monitor nonlocal maintenance and diagnostic activities.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Implement multi-factor authentication and replay resistance in the establishment of nonlocal maintenance and diagnostic sessions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Terminate session and network connections when nonlocal maintenance is completed.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.7.6. Maintenance Personnel

a. Establish a process for maintenance personnel authorization.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Maintain a list of authorized maintenance organizations or personnel.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8. Media Protection

3.8.1. Media Storage

Physically control and securely store system media that contain CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.2. Media Access

Restrict access to CUI on system media to authorized personnel or roles.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.3. Media Sanitization

Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.4. Media Marking

Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.5. Media Transport

a. Protect and control system media that contain CUI during transport outside of controlled areas.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Maintain accountability of system media that contain CUI during transport outside of controlled areas.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Document activities associated with the transport of system media that contain CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.6. Withdrawn

Addressed by 03.13.08.

3.8.7. Media Use

a. Restrict or prohibit the use of [Assignment: organization-defined types of system media].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Prohibit the use of removable system media without an identifiable owner.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.8.8. Withdrawn
Incorporated into 03.08.07.

3.8.9. System Backup – Cryptographic Protection
a. Protect the confidentiality of backup information.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI at backup storage locations.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.9. Personnel Security

3.9.1. Personnel Screening
a. This Screen individuals prior to authorizing access to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.9.2. Personnel Termination and Transfer

a. When individual employment is terminated:
   1. Disable system access within [Assignment: organization-defined time period],
   2. Terminate or revoke authenticators and credentials associated with the individual, and
   3. Retrieve security-related system property.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. When individuals are reassigned or transferred to other positions in the organization:
   1. Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility, and
   2. Modify access authorization to correspond with any changes in operational need.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10. Physical Protection

3.10.1. Physical Access Authorizations

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Issue authorization credentials for facility access.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Review the facility access list [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Remove individuals from the facility access list when access is no longer required..

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.2. Monitoring Physical Access

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.3. Withdrawn

Incorporated into 03.10.07.

3.10.4. Withdrawn

Incorporated into 03.10.07.

3.10.5. Withdrawn

Incorporated into 03.10.07.

3.10.6. Alternate Work Site

a. Determine alternate work sites allowed for use by employees.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Employ the following security requirements at alternate work sites: [Assignment: organization-defined security requirements].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.7. Physical Access Control

a. Enforce physical access authorizations at entry and exit points to the facility where the system resides by:
   1. Verifying individual physical access authorizations before granting access to the facility and
   2. Controlling ingress and egress with physical access control systems, devices, or guards.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Maintain physical access audit logs for entry or exit points.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Escort visitors, and control visitor activity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Secure keys, combinations, and other physical access devices.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

e. Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.10.8. Access Control for Transmission

Control physical access to system distribution and transmission lines within organizational facilities.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.11. Risk Assessment

3.11.1. Risk Assessment

a. Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Update risk assessments [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.11.2. Vulnerability Monitoring and Scanning

a. Monitor and scan the system for vulnerabilities [Assignment: organization-defined frequency] and when new vulnerabilities affecting the system are identified.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Remediate system vulnerabilities within [Assignment: organization-defined response times].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Update system vulnerabilities to be scanned [Assignment: organization-defined frequency] and when new vulnerabilities are identified and reported.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.11.3. Withdrawn

Incorporated into 03.11.02.

3.11.4. Risk Response

Respond to findings from security assessments, monitoring, and audits.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12. Security Assessment

3.12.1. Security Assessment

Assess the security requirements for the system and its environment of operation [Assignment: organization-defined frequency] to determine if the requirements have been satisfied.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.2. Plan of Action and Milestones

a. Develop a plan of action and milestones for the system:
   1. To document the planned remediation actions to correct weaknesses or deficiencies noted during security assessments and
   2. To reduce or eliminate known system vulnerabilities.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Update the existing plan of action and milestones based on the findings from:
   1. Security assessments,
   2. Audits or reviews, and
   3. Continuous monitoring activities.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.4. Withdrawn
Incorporated into 03.15.02.

3.12.5. Information Exchange

a. Approve and manage the exchange of CUI between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements; other types of agreements].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Document interface characteristics, security requirements, and responsibilities for each system as part of the exchange agreements.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Review and update the exchange agreements [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13. System and Communications Protection

3.13.1. Boundary Protection

a. Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Connect to external systems only through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.2. Withdrawn
Recategorized as NCO.

3.13.3. Withdrawn
Addressed by 03.01.01, 03.01.02, 03.01.03, 03.01.04, 03.01.05, 03.01.06, and 03.01.07.

3.13.4. Information in Shared System Resources
Prevent unauthorized and unintended information transfer via shared system resources.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.5. Withdrawn
Incorporated into 03.13.01.

3.13.6. Network Communications – Deny by Default – Allow by Exception
Deny network communications traffic by default and allow network communications traffic by exception.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.7. Withdrawn
Addressed by 03.01.12, 03.04.02 and 03.04.06.

3.13.8. Transmission and Storage Confidentiality

Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.9. Network Disconnect

Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.10. Cryptographic Key Establishment and Management

Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.11. Cryptographic Protection

Implement the following types of cryptography to protect the confidentiality of CUI: [Assignment: organization-defined types of cryptography].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.12. Collaborative Computing Devices and Applications

a. Prohibit the remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Provide an explicit indication of use to users physically present at the devices.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.13. Mobile Code

a. Define acceptable mobile code and mobile code technologies.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Authorize, monitor, and control the use of mobile code.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.14. Withdrawn
Technology-specific.

3.13.15. Session Authenticity
Protect the authenticity of communications sessions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.13.16. Withdrawn
Incorporated into 03.13.08.

3.14. System and Information Integrity

3.14.1. Flaw Remediation

a. Identify, report, and correct system flaws.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.2. Malicious Code Protection

a. Implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Update malicious code protection mechanisms as new releases are available in accordance with configuration management policies and procedures.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Configure malicious code protection mechanisms to:
   1. Perform scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed; an
   2. Block malicious code, quarantine malicious code, or take other mitigation actions in response to malicious code detection.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.3. Security Alerts, Advisories, and Directives

a. Receive system security alerts, advisories, and directives from external organizations on an ongoing basis.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Generate and disseminate internal system security alerts, advisories, and directives, as necessary.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.4. Withdrawn
Incorporated into 03.14.02.

3.14.5. Withdrawn
Addressed by 03.14.02.

3.14.6. System Monitoring

a. Monitor the system to detect:
   1. Attacks and indicators of potential attacks and
   2. Unauthorized connections.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Identify unauthorized use of the system.
Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.14.7. Withdrawn
Incorporated into 03.14.06.

3.14.8. Information Management and Retention
Manage and retain CUI within the system and CUI output from the system in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.15. Planning

3.15.1. Policy and Procedures

a. Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update policies and procedures [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.15.2. System Security Plan

a. Develop a system security plan that:
   1. Defines the constituent system components;
   2. Identifies the information types processed, stored, and transmitted by the system;
   3. Describes specific threats to the system that are of concern to the organization;
   4. Describes the operational environment for the system and any dependencies on or connections to other systems or system components;
   5. Provides an overview of the security requirements for the system;
   6. Describes the safeguards in place or planned for meeting the security requirements;
   7. Identifies individuals that fulfill system roles and responsibilities; and
   8. Includes other relevant information necessary for the protection of CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update the system security plan [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Protect the system security plan from unauthorized disclosure.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.15.3. Rules of Behavior

a. Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Provide rules to individuals who require access to the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

d. Review and update the rules of behavior [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.16. System and Services Acquisition

3.16.1. Security Engineering Principles

Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.16.2. Unsupported System Components

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.16.3. External System Services

a. Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.17. Supply Chain Risk Management

3.17.1. Supply Chain Risk Management Plan

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

c. Protect the supply chain risk management plan from unauthorized disclosure.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.17.2. Acquisition Strategies, Tools, and Methods

Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.17.3. Supply Chain Requirements and Processes

a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined security requirements].

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

SIGNATORY AUTHORITY

I have reviewed the System Security Plan (SSP) for <Insert Name>, and have determined that the requirements and security controls selected, and their implementation are accurate to the best of my knowledge:

Approved By:

_____ _____
External Service Provider Representative Date

Approved By:

_____ _____
_____SSA – Security Authorization Manager Date

4. RECORD OF CHANGES

Date	Description	Made By:
10-15-2024	Draft	Oyedeji Ojo -SSA

EXHIBIT C

Social Security Administration (SSA)

SYSTEM SECURITY PLAN (SSP)

FOR

SSA ESP 53 Template v1

Confidentiality: **Low**

Integrity: **Low**

Availability: **Low**

System Impact Level:

Published Date: 13 March 2024

Prepared For

Office of Information Security

REVISION HISTORY

Name	Date	Change

TABLE OF CONTENTS

1 PURPOSE

This System Security Plan provides an overview of the security requirements for the SSA ESP 53 Template v1 and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed, or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity, and availability of the data transmitted, processed or stored by SSA ESP 53 Template v1.

The security safeguards implemented for SSA ESP 53 Template v1 meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures, and practices.

2 SYSTEM IDENTIFICATION

- System Name/Version Number: SSA ESP 53 Template v1/The project version was not specified for the system.
- Acronym: SSA ESP 53 Template v1
- EA Number: A project tracking number was not assigned to the system.
- System Type: Not Specified
- Agency Operated or Contractor Operated:
- PII Data (Yes/No): No
- E-Authentication Application (Yes/No): No
- Federal Tax Information (FTI) (Yes/No): No

3 INFORMATION SYSTEM CATEGORIZATION

3.1 Information Types

This section describes how the information types used by the information system are categorized for confidentiality, integrity, and availability sensitivity levels.

The following tables identify the information types that are input, stored, processed, and/or output from SSA ESP 53 Template v1. The selection of the information types is based on guidance provided by Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office Business Reference Model 2.0 and Federal Information Processing Standards (FIPS) Pub 199, Standards for Security Categorization of Federal Information and Information Systems which is based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

Information Type	Confidentiality	Integrity	Availability
Information Sharing (M-M-M)	Moderate	Moderate	Moderate

3.2 Security Objectives Categorization (FIPS 199)

Based on the information provided in section 3.1 Information Types, SSA ESP 53 Template v1 defaults to the below high-water mark.

Confidentiality: **Low**

Integrity: **Low**

Availability: **Low**

4 PROJECT PERSONNEL

The following individuals are identified as the system owner or functional proponent/advocate for this system.

Name	Role	Email	Phone Number
Not Specified	Not Specified	Not Entered	Not Entered

5 LEVERAGED AUTHORIZATIONS

5.1 Authorization to Operate (ATO)

The SSA ESP 53 Template v1 Not Specified leverage the authority of a pre-existing Federal Entity. ATOs leveraged by SSA ESP 53 Template v1 are listed in the table that follows.

Information System Name	Federal Entity	Authorization Status	Expiration Date

5.2 FedRAMP

The SSA ESP 53 Template v1 Not Specified leverage a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by SSA ESP 53 Template v1 are listed in the table that follows.

Information System Name	Service Provider Owner	Expiration Date

6 SYSTEM INFORMATION

6.1 System Description

General Description of the System Not Specified

6.1.1 Architecture Description & Diagram

6.1.2 Network Description & Diagram

6.1.3 Dataflow Description & Diagram

6.2 System User Groups

All personnel have their status categorized with a sensitivity level in accordance with PS-2.

Category	Organization	Subsystem Name	Interface	Authentication	User Groups	Authorized Privileges	Functions Performed	Internal/External
User	Not Entered	N/A	Not Specified	Not Specified	Users	Not Specified	User Functions	Not Specified
Administrator	Not Entered	N/A	Not Specified	Not Specified	Administrators	Not Specified	Administrative Functions	Not Specified

There are currently internal personnel and external personnel. Within one year, it is anticipated that there will be internal personnel and external personnel.

7 SYSTEM ENVIRONMENT AND INVENTORY

When completed, SSA will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial Plan of Actions & Milestones (POA&M)
- Quarterly Continuous Monitoring (POA&M or as a separate document)

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 5 CM-8.

7.1 System Environment

Location	City	State
ACI-AWS	Not Entered	Not Entered
E-Vault (E-V)	Not Entered	Colorado
Kansas City Service Delivery Point (KS SDP)	Kansas City	Missouri
National Support Center (NSC)	Urbana	Maryland
Richmond Service Delivery Point (RI SDP)	Richmond	California
Secondary Support Center (SSC)	Durham	North Carolina

7.2 Equipment Inventory

7.2.1 Hardware

Hostname	Manufacturer/Model	Operating System/Version	Function

Note: IPv4 and IPv6 are only entered if applicable.

7.2.2 Software

Name	Version	Vendor	Use/Description

7.3 Ports, Protocols, and Services

Entity	Description/Service	Direction	Service	TCP/UDP	Port Number
Not Specified	Not Specified	Not Specified	Not Specified	Not Specified	

8 SYSTEM INTERCONNECTIONS

8.1 Internal Connections

System Acronym	System Name	Data Sharing Method	Data Type	Data Description	Security Categorization
Not Specified	Not Specified	Not Specified	Not Specified	Not Specified	Not Specified

8.2 External Connections

System Acronym	System Name	Data Sharing Method	Data Type	Data Description	Security Categorization
Not Specified	Not Specified	Not Specified	Not Specified	Not Specified	Not Specified

9 IMPLEMENTATION STATEMENTS

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
AC-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.d.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.d.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.d.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.h.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
AC-2.h.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.h.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.i.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.i.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.i.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.j	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.k	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-2.l	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-7.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-7.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.a.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
AC-8.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-8.c.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-14.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-14.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-17.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-17.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-18.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-18.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-19.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-19.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-20.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-20.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-20.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-22.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-22.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-22.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AC-22.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
AT-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-2(2)	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low impact.
AT-2.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-2.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-3.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-3.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AT-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
AT-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-2.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-3.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-3.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-3.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
AU-3.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-6.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-8.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-8.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-9.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-9.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-11	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-12.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-12.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
AU-12.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
CA-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.b.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.b.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.b.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-2.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-3.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
CA-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-6.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-6.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-6.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-6.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7(4).a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7(4).b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7(4).c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-7.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-9.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
CA-9.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-9.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CA-9.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-2.b.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-2.b.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-2.b.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-5	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low impact.
CM-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
CM-6.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-6.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-7.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-7.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-8.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-8.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-8.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-8.a.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-8.a.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-8.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-10.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-10.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-10.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-11.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-11.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CM-11.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
CP-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.a.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
CP-2.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-2.h	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-3.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-3.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-3.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-9.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-9.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-9.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-9.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
CP-10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
IA-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-2(1)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-2(2)	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low impact.
IA-2(8)	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low impact.
IA-2(12)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
IA-5(1).f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5(1).h	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.h	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-5.i	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-8(1)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-8(2).a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
IA-8(2).b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-8(4)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IA-11	System-Specific	Not Entered	Not Assigned	-	-	-	-	IA (Identification and Authentication) controls and additional control enhancements are not required.
IR-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-2.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-2.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-2.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
IR-5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.a.10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
IR-8.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
IR-8.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-2.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-2.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
MA-4.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MA-5.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-7.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
MP-7.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
PE-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-3.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
PE-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-6.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-8.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-8.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-8.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-12	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-13	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-14.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-14.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-15	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-16.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PE-16.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
PL-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.11	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.12	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.13	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.14	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.a.15	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
PL-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-2.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4(1).a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4(1).b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4(1).c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PL-11	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
PS-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-3.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-4.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-5.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-5.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-6.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-6.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
PS-6.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-6.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-7.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-7.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-7.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-7.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-7.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-8.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-8.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
PS-9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
RA-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3(1).a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3(1).b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-3.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5(2)	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low impact.
RA-5(11)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.b.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.b.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
RA-5.b.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-5.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
RA-7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-3.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
SA-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-3.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4(10)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.h	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-4.i	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.a.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.b.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.b.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
SA-5.b.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-5.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-8	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low impact.
SA-9.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-9.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-9.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SA-22.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SA-22.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SC-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
SC-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-7.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-7.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-7.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-12	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-13.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-13.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-15.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-15.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-20.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-20.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-21	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-22	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SC-39	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
SI-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-2.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-3.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-3.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-3.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-3.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.a.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
SI-4.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.e	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.f	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-4.g	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-5.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-5.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-5.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-5.d	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SI-12	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-1.a.1.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	The system is categorized as low or moderate-impact.
SR-1.a.1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-1.a.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-1.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-1.c.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-1.c.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-2(1)	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-2.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
SR-2.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-2.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-3.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-3.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-3.c	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
SR-5	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-8	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-10	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-11(1)	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-11(2)	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-11.a	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-11.b	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.
SR-12	System-Specific	Not Entered	Not Assigned	-	-	-	-	SA (System and Services Acquisition) controls and additional control enhancements are not required.

LAWS, REGULATIONS, STANDARDS AND GUIDANCE

- Computer Fraud and Abuse Act, 18 U.S.C. 1030
- E-Government Act (Public Law 107-347), Title III, Federal Information Security Modernization Act (FISMA)
- Federal Information System Controls Audit Manual (FISCAM)
- Federal Information Security Modernization Act of 2014 (FISMA 2014)
- Freedom of Information Act 5 U.S.C 552
- Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection
- Information Security Policy (ISP) for the Social Security Administration (SSA) Handbook
- NIST FIPS 140-2, Security Requirements for Cryptographic Modules
- NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors
- NIST SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-27 Rev. A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST SP 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-60 Vol. 1 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories

- NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide
- NIST SP 800-63-3, Digital Identity Guidelines
- NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle
- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-145, The NIST Definition of Cloud Computing
- OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act
- OMB Circular A-123, Management's Responsibility for Internal Control
- OMB Circular A-130, Managing Information as a Strategic Resource
- OMB Federal Enterprise Architecture Framework Version 2
- OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
- OMB M-04-04, E-Authentication Guidance for Federal Agencies
- OMB M-06-16, Protection of Sensitive Agency Information
- OMB M-17-15, Rescission of Memoranda Relating to Identity Management
- Privacy Act of 1974, 5 U.S.C 552.a
- Records Management by Federal Agencies, 44 U.S.C. 31
- Trade Secrets Act, 18 U.S.C. 1905, Disclosure of confidential information generally

ACRONYMS

Acronym	Definition
3PAO	Third-Party Assessment Organization
AC	Associate Commissioner
AC	Access Control
ACL	Access Control List
ACTR	Access Control Test Report
ALM	Application Lifecycle Management
AMB	Access Management Branch
AO	Authorizing Official
APM	Application Portfolio Management
APP	Application
ARB	Architecture Review Board
AT	Awareness Training
ATO	Authorization to Operate
AU	Audit and Accountability
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BII	Business Identifiable Information
BITS	Batch Integration Test System
BPD	Business Process Description
BPM	Business Project Manager
BRM	Business Reference Model
BSM	Boundary Scope Memorandum
CA	Security Assessment and Authorization
CAPRS	Change Asset Problem Reporting System
CCB	Configuration Control Board
CCCP	Configuration Change Control Process
CET	Customer Engagement Tool
CI	Configuration Items
CICS	Customer Information Control System
CIO	Chief Information Officer
CIRT	Cyber Incident Response Team
CISO	Chief Information Security Officer
CM	Configuration Management
CMP	Configuration Management Plan
COOP	Continuity of Operations Plan
COPPA	Children's Online Privacy Protection Act
COR	Contracting Officer Representative
COTS	Commercial Off The Shelf
CP	Contingency Planning
CPPs	Contingency Planning Policies
CR	Change Request
CSAM	Cybersecurity Assessment and Management

Acronym	Definition
CSO	Chief Security Officer
CUI	Confidential Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DASD	Direct Access Storage Devices
DB	Database
DBMS	Database Management System
DBOPC	Division of Batch Operation Production Control
DCA	Division of Compliance and Authorization
DCS	Deputy Commissioner for Systems
DDBS	Division of Database Systems
DESEI	Division of Enterprise Software Engineering Infrastructure
DFR	Detailed Functional Requirements
DIET	Division of Integration and Environmental Testing
DIIAS	Division of Internet/Intranet Application Services
DISSAO	Division of Information Systems Security Administration and Operations
DMSS	Division of Mainframe System Software
DMZ	Demilitarized Zone
DNE	Division of Network Engineering
DOSDO	Division of Online Systems and Database Operations
DR	Disaster Recovery
DRE	Disaster Recovery Exercise
DRMA	Division of Resource Management and Acquisition
DRP	Disaster Recovery Plan
DSE	Division of Security Engineering
DSPSM	Division of Systems Performance and Service-level Management
DSS	Detailed System Specifications
DSSM	Division of Systems Storage Management
DSUSF	Division of Systems User Services and Facilities
DTO	Division of Technical Operations
EIC	Enterprise Inheritable Controls
EMATS	Emergency Memo and Tracking System
EPO	McAfee ePolicy Orchestrator
EWANS	Enterprise Wide Mainframe & Distributed Network Telecommunications Services and System
FIPS	Federal Information Processing Standards
FISCAM	Federal Information Controls Systems Audit Manual
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FTI	Federal Tax Information
FTP	File Transfer Protocol
FTP	Functional Test Plan
GSS	General Support System
HIDS	Host-based Intrusion Detection System

Acronym	Definition
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
HW	Hardware
IA	Independent Assessor
IA	Identification and Authentication
IATO	Interim Authorization to Operate
ID	Identification
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
IR	Incident Response
IRP	Incident Response Plan
IRS	Internal Revenue Service
ISA	Interconnection Security Agreement
ISCP	Information Security Contingency Plan
ISP	Information Security Policy
ISP	Internet Service Provider
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
IV&V	Independent Verification & Validation
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LIS	Low Income Subsidy
LLC	Limited Liability Company
MA	Major Application
MA	Maintenance
MDAB	Mainframe Data Assurance Branch
MKS	Mortice Kern Systems
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection
MTD	Maximum Tolerable Downtime
MTP	Master Training Plan
MySSA	My Social Security
NDA	Non-Disclosure Agreement
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standards and Technology
NMS	Network Management System
NSC	National Support Center
OASSIS	Office of Applications and Supplemental Security Income Systems
OBFM	Office of Budget, Finance, and Management
OBIS	Office of Benefit Information Systems
OEEAS	Office of Earnings, Enumeration, and Administrative Systems

Acronym	Definition
OEP	Occupant Emergency Plan
OESAE	Office of Enterprise Support, Architecture & Engineering
OFM	Office of Facilities Management
OIS	Office of Information Security
OMB	Office of Management and Budget
OOS	Office of Systems
OPD	Office of Privacy and Disclosure
ORSIS	Office of Retirement and Survivors Insurance Systems
OS	Operating System
OSES	Office of Systems Electronic Services
OSOHE	Office of System Operations and Hardware Engineering
OSRF	Online Software Release Form
OSSF	Offsite Secure Storage Facility
OSSMB	Open Systems Storage Management Branch
OTSO	Office of Telecommunications and System Operations
P&A	Planning and Analysis
PCCB	Project Configuration Control Board
PCM	Project Configuration Manager
PDA	Personal Digital Assistant
PE	Physical and Environmental Protection
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PL	Public Law
PL	Planning
PM	Program Manager
PMC	Product Monitoring and Control
POA&M	Plan of Actions and Milestones
POC	Point of Contact
PR	Problem Report
PRIDE	Project Resource Guide
PS	Personnel Security
PSA	Project Scope Agreement
PSC	Program Service Centers
PSMA	Project Scope Management Agreement
PTA	Privacy Threshold Analysis
QA2	Quality Assurance System
RA	Risk Assessment or Risk Assessor
RA	Risk Assessment
RAR	Risk Assessment Report
RMF	Risk Management Framework
ROE	Rules of Engagement
RPO	Recovery Point Objective
rPSA	Release-Specific Project Scope Agreement
RSDI	Retirement, Survivor, or Disability Insurance

Acronym	Definition
RTO	Recovery Time Objective
SA	System and Services Acquisition
SA&A	Security Assessment and Authorization
SAM	Security Authorization Manager
SAP	System Assessment Plan, Security Authorization Package
SAR	Security Assessment Report
SAS	Security Assessment Services
SBU	Sensitive But Unclassified
SC	System and Communications Protection
SCA	Security Control Assessment
SCDF	Significant Change Determination Form
SCQ	Significant Change Questionnaire
SDLC	Systems Development Lifecycle
SDP	Systems Development Plan
SEPG	Software Engineering Process Group
SI	System and Information Integrity
SIA	Security Impact Analysis
SITAR	Strategic Information Technology Assessment Review
SME	Subject Matter Expert
SO	System Owner
SOC	Security Operations Center
SORN	System of Records Notice
SP	Special Publication
SPM	System Project Manager
SR	Service Request
SRC	Systems Release Certification
SSA	Social Security Administration
SSC	Second Support Center
SSP	System Security Plan
SW	Software
UATPA	User Acceptance Test Plan Agreement
URL	Uniform Resource Locator
V-HW	Virtual Hardware
VPN	Virtual Private Network

SIGNATORY AUTHORITY

The SSP will be reviewed at least annually or whenever a significant change occurs. Modifications to the SSP must occur within Xacta 360 and be signed by all applicable parties.

Role
SAM - Security Authorization Manager

EXHIBIT D

Social Security Administration (SSA)

SYSTEM SECURITY PLAN (SSP)

FOR

SSA ESP 171 Template v1

Confidentiality: **Low**

Integrity: **Low**

Availability: **Low**

System Impact Level:

Published Date: 13 March 2024

Prepared For

Office of Information Security

REVISION HISTORY

Name	Date	Change

TABLE OF CONTENTS

1 PURPOSE

This System Security Plan provides an overview of the security requirements for the SSA ESP 171 Template v1 and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed, or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity, and availability of the data transmitted, processed or stored by SSA ESP 171 Template v1.

The security safeguards implemented for SSA ESP 171 Template v1 meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures, and practices.

2 SYSTEM IDENTIFICATION

- System Name/Version Number: SSA ESP 171 Template v1/The project version was not specified for the system.
- Acronym: SSA ESP 171 Template v1
- EA Number: A project tracking number was not assigned to the system.
- System Type: Not Specified
- Agency Operated or Contractor Operated:
- PII Data (Yes/No): No
- E-Authentication Application (Yes/No): No
- Federal Tax Information (FTI) (Yes/No): No

3 INFORMATION SYSTEM CATEGORIZATION

3.1 Information Types

This section describes how the information types used by the information system are categorized for confidentiality, integrity, and availability sensitivity levels.

The following tables identify the information types that are input, stored, processed, and/or output from SSA ESP 171 Template v1. The selection of the information types is based on guidance provided by Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office Business Reference Model 2.0 and Federal Information Processing Standards (FIPS) Pub 199, Standards for Security Categorization of Federal Information and Information Systems which is based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

Information Type	Confidentiality	Integrity	Availability
Statistical Information	Moderate	Moderate	Moderate

3.2 Security Objectives Categorization (FIPS 199)

Based on the information provided in section 3.1 Information Types, SSA ESP 171 Template v1 defaults to the below high-water mark.

Confidentiality: **Low**

Integrity: **Low**

Availability: **Low**

4 PROJECT PERSONNEL

The following individuals are identified as the system owner or functional proponent/advocate for this system.

Name	Role	Email	Phone Number
Not Specified	Not Specified	Not Entered	Not Entered

5 LEVERAGED AUTHORIZATIONS

5.1 Authorization to Operate (ATO)

The SSA ESP 171 Template v1 Not Specified leverage the authority of a pre-existing Federal Entity. ATOs leveraged by SSA ESP 171 Template v1 are listed in the table that follows.

Information System Name	Federal Entity	Authorization Status	Expiration Date

5.2 FedRAMP

The SSA ESP 171 Template v1 Not Specified leverage a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by SSA ESP 171 Template v1 are listed in the table that follows.

Information System Name	Service Provider Owner	Expiration Date

6 SYSTEM INFORMATION

6.1 System Description

General Description of the System Not Specified

6.1.1 Architecture Description & Diagram

6.1.2 Network Description & Diagram

6.1.3 Dataflow Description & Diagram

6.2 System User Groups

All personnel have their status categorized with a sensitivity level in accordance with PS-2.

Category	Organization	Subsystem Name	Interface	Authentication	User Groups	Authorized Privileges	Functions Performed	Internal/External
Administrator	Not Entered	N/A	Not Specified	Not Specified	Administrators	Not Specified	Administrative Functions	Not Specified
User	Not Entered	N/A	Not Specified	Not Specified	Users	Not Specified	User Functions	Not Specified

There are currently internal personnel and external personnel. Within one year, it is anticipated that there will be internal personnel and external personnel.

7 SYSTEM ENVIRONMENT AND INVENTORY

When completed, SSA will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial Plan of Actions & Milestones (POA&M)
- Quarterly Continuous Monitoring (POA&M or as a separate document)

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

7.1 System Environment

Location	City	State
ACI-AWS	Not Entered	Not Entered
E-Vault (E-V)	Not Entered	Colorado
Kansas City Service Delivery Point (KS SDP)	Kansas City	Missouri
National Support Center (NSC)	Urbana	Maryland
Richmond Service Delivery Point (RI SDP)	Richmond	California
Secondary Support Center (SSC)	Durham	North Carolina

7.2 Equipment Inventory

7.2.1 Hardware

Hostname	Manufacturer/Model	Operating System/Version	Function

Note: IPv4 and IPv6 are only entered if applicable.

7.2.2 Software

Name	Version	Vendor	Use/Description

7.3 Ports, Protocols, and Services

Entity	Description/Service	Direction	Service	TCP/UDP	Port Number
Not Specified	Not Specified	Not Specified	Not Specified	Not Specified	

8 SYSTEM INTERCONNECTIONS

8.1 Internal Connections

System Acronym	System Name	Data Sharing Method	Data Type	Data Description	Security Categorization
Not Specified	Not Specified	Not Specified	Not Specified	Not Specified	Not Specified

8.2 External Connections

System Acronym	System Name	Data Sharing Method	Data Type	Data Description	Security Categorization
Not Specified	Not Specified	Not Specified	Not Specified	Not Specified	Not Specified

9 IMPLEMENTATION STATEMENTS

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.1.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.11	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.12	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.13	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.14	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.15	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.16	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.1.17	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.18	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.19	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.20	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.21	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.1.22	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.2.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.2.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.2.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.3.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.3.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.4.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.5.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.5.11	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.6.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.6.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.6.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.7.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.7.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.7.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.7.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.7.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.7.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.8.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.8.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.9.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.9.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.10.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.10.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.10.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.10.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.10.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.10.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.11.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.11.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.11.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.12.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.12.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.12.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.8	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.9	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.10	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.11	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.12	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.13	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.14	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.13.15	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

Control Ref.	Control Type	Implementation Statement	Control Status	Tailored		Overlay		Additional Comments
				IN	OUT	IN	OUT	
3.13.16	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.1	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.2	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.3	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.4	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.5	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.6	System-Specific	Not Entered	Not Assigned	-	-	-	-	None
3.14.7	System-Specific	Not Entered	Not Assigned	-	-	-	-	None

LAWS, REGULATIONS, STANDARDS AND GUIDANCE

- Computer Fraud and Abuse Act, 18 U.S.C. 1030
- E-Government Act (Public Law 107-347), Title III, Federal Information Security Modernization Act (FISMA)
- Federal Information System Controls Audit Manual (FISCAM)
- Federal Information Security Modernization Act of 2014 (FISMA 2014)
- Freedom of Information Act 5 U.S.C 552
- Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection
- Information Security Policy (ISP) for the Social Security Administration (SSA) Handbook
- NIST FIPS 140-2, Security Requirements for Cryptographic Modules
- NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors
- NIST SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-27 Rev. A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-60 Vol. 1 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories

- NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide
- NIST SP 800-63-3, Digital Identity Guidelines
- NIST SP 800-64 Rev. 2, Security Considerations in the System Development Life Cycle
- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-145, The NIST Definition of Cloud Computing
- OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act
- OMB Circular A-123, Management's Responsibility for Internal Control
- OMB Circular A-130, Managing Information as a Strategic Resource
- OMB Federal Enterprise Architecture Framework Version 2
- OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
- OMB M-04-04, E-Authentication Guidance for Federal Agencies
- OMB M-06-16, Protection of Sensitive Agency Information
- OMB M-17-15, Rescission of Memoranda Relating to Identity Management
- Privacy Act of 1974, 5 U.S.C 552.a
- Records Management by Federal Agencies, 44 U.S.C. 31
- Trade Secrets Act, 18 U.S.C. 1905, Disclosure of confidential information generally

ACRONYMS

Acronym	Definition
3PAO	Third-Party Assessment Organization
AC	Associate Commissioner
AC	Access Control
ACL	Access Control List
ACTR	Access Control Test Report
ALM	Application Lifecycle Management
AMB	Access Management Branch
AO	Authorizing Official
APM	Application Portfolio Management
APP	Application
ARB	Architecture Review Board
AT	Awareness Training
ATO	Authorization to Operate
AU	Audit and Accountability
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BII	Business Identifiable Information
BITS	Batch Integration Test System
BPD	Business Process Description
BPM	Business Project Manager
BRM	Business Reference Model
BSM	Boundary Scope Memorandum
CA	Security Assessment and Authorization
CAPRS	Change Asset Problem Reporting System
CCB	Configuration Control Board
CCCP	Configuration Change Control Process
CET	Customer Engagement Tool
CI	Configuration Items
CICS	Customer Information Control System
CIO	Chief Information Officer
CIRT	Cyber Incident Response Team
CISO	Chief Information Security Officer
CM	Configuration Management
CMP	Configuration Management Plan
COOP	Continuity of Operations Plan
COPPA	Children's Online Privacy Protection Act
COR	Contracting Officer Representative
COTS	Commercial Off The Shelf
CP	Contingency Planning
CPPs	Contingency Planning Policies
CR	Change Request
CSAM	Cybersecurity Assessment and Management

Acronym	Definition
CSO	Chief Security Officer
CUI	Confidential Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DASD	Direct Access Storage Devices
DB	Database
DBMS	Database Management System
DBOPC	Division of Batch Operation Production Control
DCA	Division of Compliance and Authorization
DCS	Deputy Commissioner for Systems
DDBS	Division of Database Systems
DESEI	Division of Enterprise Software Engineering Infrastructure
DFR	Detailed Functional Requirements
DIET	Division of Integration and Environmental Testing
DIIAS	Division of Internet/Intranet Application Services
DISSAO	Division of Information Systems Security Administration and Operations
DMSS	Division of Mainframe System Software
DMZ	Demilitarized Zone
DNE	Division of Network Engineering
DOSDO	Division of Online Systems and Database Operations
DR	Disaster Recovery
DRE	Disaster Recovery Exercise
DRMA	Division of Resource Management and Acquisition
DRP	Disaster Recovery Plan
DSE	Division of Security Engineering
DSPSM	Division of Systems Performance and Service-level Management
DSS	Detailed System Specifications
DSSM	Division of Systems Storage Management
DSUSF	Division of Systems User Services and Facilities
DTO	Division of Technical Operations
EIC	Enterprise Inheritable Controls
EMATS	Emergency Memo and Tracking System
EPO	McAfee ePolicy Orchestrator
EWANS	Enterprise Wide Mainframe & Distributed Network Telecommunications Services and System
FIPS	Federal Information Processing Standards
FISCAM	Federal Information Controls Systems Audit Manual
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FTI	Federal Tax Information
FTP	File Transfer Protocol
FTP	Functional Test Plan
GSS	General Support System
HIDS	Host-based Intrusion Detection System

Acronym	Definition
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
HW	Hardware
IA	Independent Assessor
IA	Identification and Authentication
IATO	Interim Authorization to Operate
ID	Identification
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
IR	Incident Response
IRP	Incident Response Plan
IRS	Internal Revenue Service
ISA	Interconnection Security Agreement
ISCP	Information Security Contingency Plan
ISP	Information Security Policy
ISP	Internet Service Provider
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
IV&V	Independent Verification & Validation
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LIS	Low Income Subsidy
LLC	Limited Liability Company
MA	Major Application
MA	Maintenance
MDAB	Mainframe Data Assurance Branch
MKS	Mortice Kern Systems
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection
MTD	Maximum Tolerable Downtime
MTP	Master Training Plan
MySSA	My Social Security
NDA	Non-Disclosure Agreement
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standards and Technology
NMS	Network Management System
NSC	National Support Center
OASSIS	Office of Applications and Supplemental Security Income Systems
OBFM	Office of Budget, Finance, and Management
OBIS	Office of Benefit Information Systems
OEEAS	Office of Earnings, Enumeration, and Administrative Systems

Acronym	Definition
OEP	Occupant Emergency Plan
OESAE	Office of Enterprise Support, Architecture & Engineering
OFM	Office of Facilities Management
OIS	Office of Information Security
OMB	Office of Management and Budget
OOS	Office of Systems
OPD	Office of Privacy and Disclosure
ORSIS	Office of Retirement and Survivors Insurance Systems
OS	Operating System
OSES	Office of Systems Electronic Services
OSOHE	Office of System Operations and Hardware Engineering
OSRF	Online Software Release Form
OSSF	Offsite Secure Storage Facility
OSSMB	Open Systems Storage Management Branch
OTSO	Office of Telecommunications and System Operations
P&A	Planning and Analysis
PCCB	Project Configuration Control Board
PCM	Project Configuration Manager
PDA	Personal Digital Assistant
PE	Physical and Environmental Protection
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PL	Public Law
PL	Planning
PM	Program Manager
PMC	Product Monitoring and Control
POA&M	Plan of Actions and Milestones
POC	Point of Contact
PR	Problem Report
PRIDE	Project Resource Guide
PS	Personnel Security
PSA	Project Scope Agreement
PSC	Program Service Centers
PSMA	Project Scope Management Agreement
PTA	Privacy Threshold Analysis
QA2	Quality Assurance System
RA	Risk Assessment or Risk Assessor
RA	Risk Assessment
RAR	Risk Assessment Report
RMF	Risk Management Framework
ROE	Rules of Engagement
RPO	Recovery Point Objective
rPSA	Release-Specific Project Scope Agreement
RSDI	Retirement, Survivor, or Disability Insurance

Acronym	Definition
RTO	Recovery Time Objective
SA	System and Services Acquisition
SA&A	Security Assessment and Authorization
SAM	Security Authorization Manager
SAP	System Assessment Plan, Security Authorization Package
SAR	Security Assessment Report
SAS	Security Assessment Services
SBU	Sensitive But Unclassified
SC	System and Communications Protection
SCA	Security Control Assessment
SCDF	Significant Change Determination Form
SCQ	Significant Change Questionnaire
SDLC	Systems Development Lifecycle
SDP	Systems Development Plan
SEPG	Software Engineering Process Group
SI	System and Information Integrity
SIA	Security Impact Analysis
SITAR	Strategic Information Technology Assessment Review
SME	Subject Matter Expert
SO	System Owner
SOC	Security Operations Center
SORN	System of Records Notice
SP	Special Publication
SPM	System Project Manager
SR	Service Request
SRC	Systems Release Certification
SSA	Social Security Administration
SSC	Second Support Center
SSP	System Security Plan
SW	Software
UATPA	User Acceptance Test Plan Agreement
URL	Uniform Resource Locator
V-HW	Virtual Hardware
VPN	Virtual Private Network

SIGNATORY AUTHORITY

The SSP will be reviewed at least annually or whenever a significant change occurs. Modifications to the SSP must occur within Xacta 360 and be signed by all applicable parties.

Role
SAM - Security Authorization Manager

EXHIBIT E

Attachment A. (GAM 15.02) Worksheet for Reporting Loss or Potential Loss of PII

The "Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information" is intended to assist you to quickly organize and report the needed information about the potential incident.

1. Information about the individual making the report to the NNSC:

Name:					
Position:					
Deputy Commissioner Level Organization:					
Phone Numbers:					
Work:		Cell:		Home/Other:	
Email Address:					
Check one of the following:					
Management Official		Security Officer		Non-Management	

2. Information about the data that was lost/stolen:

Describe what was lost or stolen (e.g., case file, MBR data):

Which element(s) of PII did the data contain?

Name		Bank Account Info	
SSN		Medical/Health Information	
Date of Birth		Benefit Payment Info	
Place of Birth		Mother's Maiden Name	
Address		Other (describe):	

Estimated volume of records involved:

3. How was the data physically stored, packaged and/or contained?

Paper or Electronic? (Circle one):

If Electronic, what type of device?

Laptop		USB Drive		Backup Tape		Blackberry	
Workstation		Server		CD/DVD		Mobile Phone #	
Hard Drive		Floppy Disk		Cell (not Blackberry)			
Other (describe):							

Additional Questions if Electronic:

								Yes	No	Not Sure
a. Was the device encrypted?										
b. Was the device password protected?										
c. If a laptop, was a VPN SmartCard lost?										
d. If laptop, powerstate when	Off		Sleep		Hibernate		Not			

lost?							Sure	
Cardholder's Name:								
Cardholder's SSA logon PIN:								
Hardware Make/Model:								
Hardware Serial Number:								

Additional Questions if Paper:

	Yes	No	Not Sure
a. Was the information in a locked briefcase?			
b. Was the information in a locked cabinet or drawer?			
c. Was the information in a locked vehicle trunk?			
d. Was the information redacted?			
e. Other circumstances:			

4. If the employee/contractor who was in possession of the data or to whom the data was assigned is not the person making the report to the NNSC (as listed in #1), information about this employee/contractor:

Name:					
Position:					
Deputy Commissioner Level Organization:					
Phone Numbers:					
Work:		Cell:		Home/Other:	
Email Address:					

5. Circumstances of the loss:

a. When was it lost/stolen:

b. Brief description of how the loss/theft occurred:

c. When was it reported to SSA management official (date and time)?

6. Have any other SSA components been contacted? If so, who? (Include deputy commissioner level, agency level, regional/associate level component names)

7. Which reports have been filed? (include FPS, local police, and SSA reports)

Report Filed	Yes	No	Report Number
Federal Protective Service			
Local Police			
OIG			

	Yes	No
SSA-3114 (Incident Alert)		
SSA-342 (Report of Survey)		
Security Assessments and Funded Enhancements (SAFE)		

Other (describe)

8. **Other pertinent information (include actions underway as well as any contacts with other agencies, law enforcement or the press):**

EXHIBIT F

GENERAL RECORDS SCHEDULE 4.2: Information Access and Protection Records

This schedule covers records created in the course of agencies (1) responding to requests for access to Government information and (2) protecting information that is classified or controlled unclassified, or contains personal data that is required by law to be protected.

Agencies must offer any records created prior to January 1, 1921, to the National Archives and Records Administration (NARA) before applying disposition instructions in this schedule.

Item	Records Description	Disposition Instruction	Disposition Authority
001	**FOIA, Privacy Act, and classified documents administrative records.** Records on managing information access and protection activities. Records include: • correspondence related to routine implementation of the FOIA and Privacy Act and administration of document security classification • associated subject files • feeder and statistical reports **Exclusion:** This item does not cover records documenting policies and procedures accumulated in offices having agency-wide responsibilities for FOIA, Privacy Act, and classified documents. These records must be scheduled by the agency on an agency-specific schedule.	**Temporary.** Destroy when 3 years old, but longer retention is authorized if needed for business use.	DAA-GRS-2019-0001-0001
010	**General information request files.** Requests for information, publications, photographs, and other information involving no administrative action, policy decision, or special compilations or research. Also includes acknowledgements, replies, and referrals of inquiries to other offices for response.	**Temporary**. Destroy when 90 days old, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0001
020	**Access and disclosure request files**. Case files created in response to requests for information under the Freedom of Information Act (FOIA), Mandatory Declassification Review (MDR) process, Privacy Act (PA), Classification Challenge, and similar access programs, and completed by: • granting the request in full • granting the request in part • denying the request for any reason including: o inability to fulfill request because records do not exist o inability to fulfill request because request inadequately describes records	**Temporary**. Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later, but longer retention is authorized if required for business use.	DAA-GRS-2016-0002-0001

Security and Privacy Awareness Training
Contractor / Affiliate Personnel Security Certification

Purpose:

This training document is to be signed by contractor, subcontractor, or affiliate personnel, and those acting on behalf of the Social Security Administration (SSA) who have been granted access to SSA information and information systems to certify that they have received and understand SSA Information Security and Privacy Awareness Training detailed below.

Background:

SSA is vital to the economic security of the United States. In the performance of their duties in support of SSA's mission, all contractors, subcontractors, affiliates, and those acting on behalf of SSA who have been granted access to SSA information systems, hereafter referred to as "Authorized Users(s)," are responsible for protecting such information and information systems (e.g., hardware, software/applications, federal information/data, network, people) throughout the entire information life cycle, including collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Federal information includes information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Security awareness training is required for Authorized Users, per Section 44 USC 3554 of the Federal Information Security Modernization Act of 2014 (FISMA). Failure to follow prescribed rules or misuse of federal information and information systems can lead to criminal penalties, including fines and imprisonment, and disciplinary actions according to the contract and/or agreement under which I am performing work for SSA.

I understand that SSA maintains a variety of sensitive information about the agency's operations and programs, which may be information pertaining to program (e.g., information about SSA's clients) or non-program (e.g., administrative and personnel records) matters. I understand that SSA may authorize me to have access to federal information and information systems and that my access to and use of such information and information systems must be in accordance with the provisions of the contract and/or agreement under which I am performing work for SSA.

I understand that the terms in the contract and/or agreement under which I am performing work for SSA take precedence over this document. I understand that any questions I may have concerning authorization(s) to access SSA information and information systems should be directed in accordance with the terms of the contract and/or agreement. I have read, understand, and agree to the following conditions:

Insider Threat

An insider threat is someone with authorized access who uses that access, intentionally or unintentionally, to harm the security of the Agency or the Nation. The individual with authorized access may attempt to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities.

- If I observe a potential insider threat, **I will** report the incident to SSAITP@ssa.gov and, as appropriate, in accordance with the personally identifiable information and incident reporting requirements in the contract or agreement under which I am working.
- **I will** safeguard federal information and information systems from exploitation, compromise, espionage, terrorism, or other unauthorized use and disclosure.

Malware, Remote Access, and Mobile Device Security

Malware encompasses malicious software, programs, files, and/or code in the form of virus, ransomware, and spyware that cause damage to information systems and data. SSA defends against malware using antivirus programs, intrusion detection systems, and social engineering training among other methods. Routine software and security updates ensure SSA devices are up to date with the latest malware protection.

When I have been granted an SSA device to perform work for the agency, the following requirements apply:

- In order to ensure my SSA device receives the necessary software and security updates**, I will** remain connected to SSANet using the agency's Virtual Private Network throughout my workday**, I will** keep my workstation plugged in and powered on, and **I will** restart my workstation at least once a week and at the end of each workday, logging off from the CTRL+ALT+DELETE screen unless further guidance is issued.

- **I will not** store federal information on personally owned media devices or, connect non-SSA approved and issued personal Bluetooth devices to an SSA device.

- **I will not** alter SSA devices, disable security settings, or download or install unauthorized software onto SSA devices.

- **I will** follow the security and safety requirements of any alternative worksite agreement and all contract or agreements related to non-SSA worksites.

- **I will not** print any material that contains federal information at an unapproved location. **I will** protect SSA devices at all times, to include while on travel, at any alternative worksite, and any approved non-SSA worksite.

Secure Browsing and Social Media

Attackers use social data mining techniques to gather information about an individual or organization in public or social settings, including social media. SSA social media accounts are not official SSA websites, but rather the department's presence on third-party service providers' platforms, which means SSA has limited control over how each platform uses personal data provided by users.

- **I will not** transmit, store, or process federal information on non-SSA owned and operated sites, including social media, third party online forums, third-party collaboration tools or sites, social networking sites, any other non-SSA-hosted sites, or unapproved third-party data storage providers unless explicitly authorized to do so.

- **I will not** share programming code used for federal information systems with unauthorized individuals including but not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

- **I will not** use federal information systems to browse or access information about myself, my children, other family members, co-workers or former co-workers, acquaintances, and/or friends.

Secure Email and Fax Use

Email is an official business communication tool and users must use it in a responsible, secure, and lawful manner. When using SSA email, to protect agency systems and those who receive email from me:

- **I will** use business communication tools including SSA email in a responsible, secure, and lawful manner.
- **I will not** send or forward Personally Identifiable Information (PII) to or from a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List.
- **I will not** copy or blind copy work-related email to a personal, non-SSA email address.
- **I will not** send or forward chain letters or other unauthorized mass mailings.
- **I will not** configure my SSA email account to automatically forward work-related email to an outside (non-SSA, non-secure) address.
- If I receive an email intended for someone else, **I will** immediately notify the sender and delete or destroy the misdirected message.

A fax is an official business communication tool and users must use it in a responsible, secure, and lawful manner. When using an SSA fax, to protect agency systems and those who receive faxes from me:

- **I will** use business communication tools including SSA fax in a responsible, secure, and lawful manner.
- **I will** use a cover sheet that notes the sensitivity of the material and follow all Controlled Unclassified Information (CUI) labeling requirements.
- **I will not** leave fax machines unattended when transmitting.
- **I will** transmit faxes to the intended recipient, when possible, using pre-programmed fax numbers.
- **I will not** use SSA's fax system to create or distribute disruptive or offensive messages.
- If I receive a fax by mistake, **I will** notify the sender. To the extent possible, **I will not** read the fax's contents. **I will** destroy the misdirected message.

Security Incident Reporting

Security incidents involve any attempted or actual authorized access, use, disclosure, modification, or destruction of information. Examples include malicious or unauthorized intrusion or access, virus attacks, phishing, vishing, supply chain threats, foreign intelligence threats, insider threats, and loss of PII.

- If I suspect or confirm the loss or theft of any sensitive information, including PII, **I will** report it within one hour to my supervisor, manager, contracting officer's representative and/or contracting officer's technical representative or another designated official. If those individuals are not available, **I will** use the PII Loss Reporting Tool to report any loss or theft of any sensitive information or PII.
- If I observe a suspected systems intrusion attempt or other security-related incident, **I will** report the incident within 15 minutes of discovery to SOC@ssa.gov.
- If I am the targeted victim of a phishing (suspicious email) attempt, **I will** report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- If I am the target of a vishing (suspicious phone call) attempt, **I will** report the incident within 15 minutes of discovery to SOC@ssa.gov.
- If I observe a potential insider threat, **I will** report the incident to SSAITP@ssa.gov. If I observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, **I will** report the incident to the Office of the Inspector General in accordance with published policy.

Social Engineering

Vishing is the practice of tricking you, over the phone, into revealing information to an unauthorized individual or performing actions on your workstation that may compromise the security of SSA.

- **I will** avoid vishing attempts by validating a caller's identity and purpose.
- If I am unable to validate the caller's identity, **I will** hang up and call back using a number I know to be correct.

Phishing is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.

- **I will** avoid phishing attempts by verifying the email sender.
- **I will** be suspicious when receiving emails from individuals I do not know or have not heard from in a long time.
- **I will** never respond to requests for PII or send password information in an email.
- **I will** only release information if I am confident of an individual's identity and right to receive it.

Unauthorized Access and Prohibited Behavior

Unauthorized access to federal information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Federal information system users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time, including accessing the Internet using E-mail.

- **I will not** inspect, access, or attempt to access any federal information that SSA has not expressly authorized me to access.
- **I will not** release or disclose any federal information to any unauthorized person, agency, or entity. **I understand** that unauthorized disclosure of federal information may lead to civil penalties and/or criminal prosecution under Federal law (e.g., The Privacy Act of 1974, 5 U.S.C. 552a; SSA's regulations at 20 C.F.R. Part 401; The Social Security Act, 42 U.S.C. 1306 (a); and 5 U.S.C. Section 552(i)). **I further understand** that additional privacy and disclosure protections may apply to certain types of SSA information including Federal Tax Information (i.e., earnings information), which may be subject to additional penalties under sections 6103, 7213, 7213A, and 7431 of the Internal Revenue Service (IRS) Code (Title 26 of the United States Code).
- **I will** follow all access, retention, and/or destruction requirements in the contract and/or agreement under which I am authorized to access federal information. **I understand** that such requirements may require me to cease access to, return, or destroy federal information upon completion of my work for SSA or termination of my contract and/or agreement that authorized my access to federal information.
- **I will not** take federal information off-site, unless expressly authorized to do so by contract and/or agreement or other written authorization from SSA. If SSA authorizes me to take federal information off-site, I agree to safeguard all such information in accordance with agency policy and standards and the requirements of the contract and/or agreement under which I am performing work so that no unauthorized person, agency, or entity can access federal information.
- **I will** keep confidential any third-party proprietary information that may be entrusted to me as part of the contract and/or agreement, including safeguarding such information from unauthorized access and not disclosing or releasing such information unless expressly authorized to do so.
- **I will** follow all requirements in the contract and/or agreement under which I am performing work for SSA, includingbut not limited to those governing confidential information or PII.
- **I will** only use my access to federal information and information systems for the performance of my official duties.

Contractor Employee Name (Print/Type)	Date (MM/DD/YYYY)
Contractor Employee Signature (Sign)	

Contract Number	Company Name (Print/Type)
Company Point Of Contact (Print/Type)	Company Point of Contact Phone Number

Privacy Act
Collection and Use of Personal Information

42 U.S.C. § 904(a); 20 C.F.R. § 401.90; 44 U.S.C. §§ 3541-3549; 41 C.F.R. Chapter 101; 5 U.S.C. § 552a(e)(9)-(10); and Executive Order 13488 of the Social Security Act, as amended, allow us to collect this information. Furnishing this information to the Social Security Administration (SSA) is voluntary. However, failing to provide this information may affect your ability to access Federal information and information systems, which is a condition of the contract under which you are performing work for SSA (SSA contract). Not providing this information also could prevent us from issuing you a PIV credential and/or authorizing you to access SSA's network, one or both of which may be conditions of your SSA contract. Failure to follow prescribed rules or misuse of SSA information and information systems could lead to removal from duty from your SSA contract.

We will use the information you provide to grant you access to Federal information and information systems. We may also share your information for the following purposes, called routine uses:

- To contractors and other Federal agencies, as necessary, for assisting SSA in the efficient administration of its programs. We disclose information under this routine use only in situations in which SSA may enter into a contractual or similar agreement with a third party to assist the accomplishing an agency function relating to this system of records; and

- To student volunteers, individuals working under a personal services contract, and other workers who individuals performing functions for SSA but technically do not having the status of Federal agency employees, when they are performing work for SSA, as authorized by law, and if they need access to personally identifiable information (PII) in SSA the records in order to perform their assigned agency functions.

In addition, we may share this information in accordance with the Privacy Act and other Federal laws. For example, where authorized, we may use and disclose this information in computer matching programs, in which our records are compared with other records to establish or verify a person's eligibility for Federal benefit programs and for repayment of incorrect or delinquent debts under these programs.

A list of additional routine uses is available in our Privacy Act System of Records Notice (SORN) 60-0361, entitled Identity Management System, as published in the Federal Register (FR) on November 3, 2006, at 71 FR 64751. Additional information, and a full listing of all our SORNs, is available on our website at www.ssa.gov/privacy.

Item	Records Description		Disposition Instruction	Disposition Authority
	○ inability to fulfill request because search or reproduction fees are not paid • final adjudication on appeal to any of the above original settlements • final agency action in response to court remand on appeal Includes: • requests (either first-party or third-party) • replies • copies of requested records • administrative appeals • related supporting documents (such as sanitizing instructions) **Note 1**: Record copies of requested records remain covered by their original disposal authority, but if disposable sooner than their associated access/disclosure case file, may be retained under this item for disposition with that case file. **Note 2**: Agencies may wish to retain redacted copies of requested records for business use after the rest of the associated request case file is destroyed.			
030	**Information access and protection operational records**.	**Records tracking and controlling access to protected information.** Includes: • records documenting receipt, internal routing, dispatch, or destruction of classified and controlled unclassified records • tracking databases and other records used to manage overall access program • requests and authorizations for individuals to have access to classified and controlled unclassified records and information **Note**: Records documenting individuals' security clearances are covered under GRS 5.6, items 180 and 181.	**Temporary**. Destroy 2 years after last form entry, reply, or submission; or when associated documents are declassified, decontrolled, or destroyed; or when an individual's authorization expires; whichever is appropriate. Longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0002
031		**Access control records.** Includes: • safe and padlock combinations • names or other personal identifiers of individuals who know combinations	**Temporary**. Destroy when superseded or obsolete, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0020

Item	Records Description		Disposition Instruction	Disposition Authority
		• comparable data used to control access into classified document containers		
032		**Records relating to classified or controlled unclassified document containers.** Includes forms placed on safes, cabinets, or vaults that record opening, closing, and routine checking of container security, such as SF-701 and SF-702. **Note**: Forms involved in investigations are not covered by this item. They are instead retained according to the schedule item for records of the investigation.	**Temporary**. Destroy 90 days after last entry on form, but longer retention is authorized if required for business use.	DAA-GRS-2016-0002-0003
040	**Records of accounting for and controlling access to records requested under FOIA, PA, and MDR**. Records documenting identity of, and internal routing, control points, and accountability for information to which access has been requested. Includes: • forms, registers, ledgers, logs, and tracking systems documenting requester identity and contact information, request date, and nature or purpose of request • inventories • forms accompanying documents to ensure continuing control, showing names of people handling the documents, inter-office routing, and comparable data • agent and researcher files		**Temporary**. Destroy 5 years after date of last entry or final action by agency, as appropriate, but longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0003
050	**Privacy Act accounting of disclosure files**. Files maintained under the provisions of 5 U.S.C. §552a(c) for an accurate accounting of the date, nature, and purpose of each disclosure of a record to any person or to another agency. Includes: • forms with the subject individual's name • records of the requester's name and address • explanations of the purpose for the request • date of disclosure • proof of subject individual's consent		**Temporary**. Dispose of in accordance with the approved disposition instructions for the related subject individual's records, or 5 years after the disclosure for which the accountability was made, whichever is later.	NC1-64-77-1 item 27

Item	Records Description		Disposition Instruction	Disposition Authority
060	**Erroneous release records**. Files relating to the inadvertent release of privileged information to unauthorized parties, containing information the disclosure of which would constitute an unwarranted invasion of personal privacy. Includes: • requests for information • copies of replies • all related supporting documents May include: • official copy of records requested or copies	**Records filed with the record-keeping copy of the erroneously released records.**	**Temporary**. Follow the disposition instructions approved for the released record copy or destroy 6 years after the erroneous release, whichever is later.	DAA-GRS-2015-0002-0001
061		**Records filed separately from the record-keeping copy of the released records.**	**Temporary**. Destroy 6 years after the erroneous release, but longer retention is authorized if required for business use.	DAA-GRS-2015-0002-0002
065	**Privacy complaint files**. Records of privacy complaints (and responses) agencies receive in these categories: • process and procedural (consent, collection, and appropriate notice) • redress (inquiries seeking resolution of difficulties or concerns about privacy matters not specifically outlined in the Privacy Act) • operational (inquiries regarding Privacy Act matters but not including Privacy Act requests for access and/or correction) • complaints referred to another organization		**Temporary**. Destroy 3 years after resolution or referral, as appropriate, but longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0004
070	**Agency reports to the Congress, Department of Justice, or other entities regarding FOIA, MDR, PA, and similar access and disclosure programs.** **Note**: This item does not apply to summary reports incorporating government-wide statistics. These must be scheduled separately by the summarizing agent.		**Temporary**. Destroy 2 years after date of report, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0006
080	**Legal and regulatory compliance reporting records.** Reports prepared in compliance with Federal laws and regulations, such as the E-Government Act (Public Law 107-347), Federal Information Security Modernization Act of 2014, and Title V (Confidential Information	**Annual reports by agency CIO, Inspector General, or Senior Agency Official for Privacy.** **Legal citation**: OMB M-07-16.	**Temporary**. Destroy 5 years after submission of report, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0022

Item	Records Description		Disposition Instruction	Disposition Authority
081	Protection and Statistical Efficiency Act), as codified in 44 U.S.C. §101.	**All other agency reports and internal reports by individual system owners to the Senior Agency Official for Privacy (SAOP).**	**Temporary**. Destroy 2 years after submission of report, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0023
090	**Privacy Act amendment request files.** Files relating to an individual's request to amend a record pertaining to that individual under 5 U.S.C. §552a(d)(2), to the individual's request for review of an agency's refusal to amend a record under 5 U.S.C. §552a(d)(3), and to any civil action or appeal brought by the individual against the refusing agency under 5 U.S.C. §552a(g). Includes: • requests to amend and to review refusal to amend • copies of agency's replies • statement of disagreement • agency justification for refusal to amend a record • appeals • related materials		**Temporary**. Destroy with the records for which amendment was requested or 4 years after close of case (final determination by agency or final adjudication, whichever applies), whichever is later. Longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0007
100	**Automatic and systematic declassification review program records**. Files related to the review of permanent records in anticipation of automatic declassification at 25, 50, or 75 years per Executive Order 13526, and the periodic review of records exempted from automatic declassification. Files include program records documenting declassification decisions.		**Temporary**. Destroy or delete 30 years after completion of review, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0008
110	**Fundamental classification guidance review files.** Reports, significant correspondence, drafts, received comments, and related materials responding to "fundamental classification guidance review" as required by Executive Order 13526 Section 1.9. **Note**: This item does not cover reports and correspondence received at the Information Security Oversight Office (ISOO).		**Temporary**. Destroy 5 years after report is submitted to ISOO, but longer retention is authorized if required for business use.	DAA-GRS-2013-0007-0011
120	**Classified information nondisclosure agreements**. Copies of nondisclosure agreements, such as SF 312, Classified Information Nondisclosure Agreement,	**Records maintained in the individual's official personnel folder.**	Apply the disposition for the official personnel folder.	

Item	Records Description		Disposition Instruction	Disposition Authority
121	signed by civilian and military personnel with access to information that is classified under standards put forth by executive orders governing security classification.	**Records maintained separately from the individual's official personnel folder.** **Legal citations:** ICD 703, Protection of Classified National Intelligence; 32 CFR 2001.80(d)(2)(vii).	**Temporary**. Destroy when 50 years old.	DAA-GRS-2015-0002-0003
130	**Personally identifiable information extracts.** System-generated or hardcopy print-outs generated for business purposes that contain Personally Identifiable Information. **Legal citation**: OMB M-07-16 (May 22, 2007), Attachment 1, Section C, bullet "Log and Verify."		**Temporary**. Destroy when 90 days old or no longer needed pursuant to supervisory authorization, whichever is appropriate.	DAA-GRS-2013-0007-0012
140	**Personally identifiable information extract logs.** Logs that track the use of PII extracts by authorized users, containing some or all of: date and time of extract, name and component of information system from which data is extracted, user extracting data, data elements involved, business purpose for which the data will be used, length of time extracted information will be used. Also includes (if appropriate): justification and supervisory authorization for retaining extract longer than 90 days, and anticipated disposition date.		**Temporary**. Destroy when business use ceases.	DAA-GRS-2013-0007-0013
150	**Privacy Act System of Records Notices (SORNs).** Agency copy of notices about the existence and character of systems of records, documenting publication in the Federal Register when the agency establishes or revises the system, per the Privacy Act of 1974 [5 U.S.C. 552a(e)(4) and 5 U.S.C. 552a(e)(11)], as amended. Also significant material documenting SORN formulation, other than Privacy Impact Assessment records (see item 161).		**Temporary**. Destroy 2 years after supersession by a revised SORN or after system ceases operation, but longer retention is authorized if required for business use.	DAA-GRS-2016-0003-0002
160	**Records analyzing Personally Identifiable Information (PII).** Records documenting whether certain privacy and data security laws, regulations, and agency policies are required; how the agency collects, uses, shares, and maintains PII; and incorporation of privacy protections into	**Records of Privacy Threshold Analyses (PTAs) and Initial Privacy Assessments (IPAs).** Records of research on whether an agency should conduct a Privacy Impact Assessment (PIA).	**Temporary**. Destroy 3 years after associated PIA is published or determination that PIA is unnecessary, but longer retention is authorized if required for business use.	DAA-GRS-2016-0003-0003

Item	Records Description		Disposition Instruction	Disposition Authority
161	records systems as required by the E-Government Act of 2002 (Public Law 107-347, section 208), the Privacy Act of 1974 (5 U.S.C. 552a), and other applicable privacy laws, regulations, and agency policies. Includes significant background material documenting formulation of final products.	**Records of Privacy Impact Assessments (PIAs).**	**Temporary**. Destroy 3 years after a superseding PIA is published, after system ceases operation, or (if PIA concerns a website) after website is no longer available to the public, as appropriate. Longer retention is authorized if required for business use.	DAA-GRS-2016-0003-0004
170	**Computer matching program notices and agreements.** Agency copy of notices of intent to share data in systems of records with other Federal, state, or local government agencies via computer matching programs, and related records documenting publication of notice in the Federal Register per the Privacy Act of 1974 [5 U.S.C. 552a(e)(12)], as amended. Also agreements between agencies, commonly referred to as Computer Matching Agreements, prepared in accordance with Office of Management and Budget Final Guidance. Includes documentation of Data Integrity Board (DIB) review and approval of matching programs and agreements, and significant background material documenting formulation of notices and agreements.		**Temporary**. Destroy upon supersession by a revised notice or agreement, or 2 years after matching program ceases operation, but longer retention is authorized if required for business use.	DAA-GRS-2016-0003-0005
180	**Virtual public access library records.** Records published by an agency on line to fulfill the requirement in 5 U.S.C. 552(a)(2)(A) through 5 U.S.C. 552(a)(2)(D) and 5 U.S.C. 552(g)(1) through 5 U.S.C. 552(g)(3) that agencies must make those records available for public inspection and copying. Includes: • final concurring and dissenting opinions and orders agencies issue when adjudicating cases • statements of policy and interpretations the agency adopts but does not publish in the *Federal Register* • administrative staff manuals and instructions to staff that affect a member of the public • copies of records requested under the Freedom of Information Act (FOIA) which, because of the nature of their subject matter, the agency determines are, or are likely to become, the subject of subsequent requests for substantially the same records or which have been requested three or more times • indexes of agency major information systems		**Temporary**. Destroy when no longer needed.	DAA-GRS-2016-0008-0001

Item	Records Description	Disposition Instruction	Disposition Authority
	• descriptions of agency major information and record locator systems • handbooks for obtaining various types and categories of agency public information **Exclusion**: This item refers only to copies an agency publishes on line for public reference. The agency record copy of such material may be of permanent value and the agency must schedule it. Not media neutral. Applies to electronic records only.		
Controlled Unclassified Information (CUI) program records. **Exclusion:** Records of the Controlled Unclassified Information Executive Agent office at the National Archives (NARA must schedule these records separately).			
190	**CUI program implementation records.** Records of overall program management. Includes: • records documenting the process of planning agency policy and procedure • agency submissions to the CUI Executive Agent of authorities (laws, Federal regulations, or Government-wide policies containing safeguarding or dissemination controls) the agency proposes to include in the CUI Registry to designate unclassified information as CUI • agency submissions to the CUI Executive Agent of proposed laws, Federal regulations, or Government-wide policies that would establish, eliminate, or modify a category of CUI, or change information controls applicable to CUI • correspondence with CUI Executive Agent **Exclusion 1**: CUI directives and formal policy documents (agencies must schedule these separately). **Exclusion 2**: Records of CUI self-inspections (GRS 5.7, item 020 covers these). **Exclusion 3**: Records of annual program reports to the CUI Executive Agent (GRS 5.7, item 050 covers these).	**Temporary**. Destroy when 7 years old, but longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0005
191	**CUI information sharing agreements.** Agreements in which agencies agree to share CUI with non-executive branch entities (*e.g.*, state and local police) and foreign entities that agree to protect the CUI.	**Temporary**. Destroy 7 years after canceled or superseded, but longer retention is	DAA-GRS-2019-0001-0006

Item	Records Description		Disposition Instruction	Disposition Authority
	Exclusion: Contracts involving CUI and contractor access to CUI; GRS 1.1, item 010 covers contracts.		authorized if required for business use.	
192	**Records of waivers of CUI requirements.** Description of and rationale for each waiver, documentation of alternate steps the agency takes to ensure it sufficiently protects the CUI covered by the waiver, and records of the agency notifying authorized recipients and the public of the waiver.		**Temporary**. Destroy when waiver is rescinded, system is no longer in use, or all affected records are destroyed, as applicable, but longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0007
193	**Records of requests for decontrol and challenges to CUI designations.** Requests to decontrol CUI or challenging a CUI marking as incorrect (either improperly assigned or lacking), responses to requests, records of adjudication, and records of dispute resolution if adjudication is appealed.	**Records filed with the record-keeping copy of the CUI-marked records.**	Follow the disposition instructions approved for the records at issue.	
194		**Records filed separately from the record-keeping copy of the CUI-marked records.**	**Temporary.** Destroy 6 years after change in CUI status, but longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0008
195	**Records of CUI misuse.** Allegations of CUI misuse, records of internal investigations, communications with and reports of findings from the CUI Executive Agent, and records of corrective actions. **Exclusion**: If the agency assigns such investigations to its Inspector General (IG), the agency schedule for IG records covers the records created in the IG office.		**Temporary**. Destroy 5 years after completing the investigation or completing all corrective actions, whichever is later, but longer retention is authorized if required for business use.	DAA-GRS-2019-0001-0009

EXHIBIT G

Security and Privacy Awareness Training
Contractor / Affiliate Personnel Security Certification

Purpose:

This training document is to be signed by contractor, subcontractor, or affiliate personnel, and those acting on behalf of the Social Security Administration (SSA) who have been granted access to SSA information and information systems to certify that they have received and understand SSA Information Security and Privacy Awareness Training detailed below.

Background:

SSA is vital to the economic security of the United States. In the performance of their duties in support of SSA's mission, all contractors, subcontractors, affiliates, and those acting on behalf of SSA who have been granted access to SSA information systems, hereafter referred to as "Authorized Users(s)," are responsible for protecting such information and information systems (e.g., hardware, software/applications, federal information/data, network, people) throughout the entire information life cycle, including collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Federal information includes information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Security awareness training is required for Authorized Users, per Section 44 USC 3554 of the Federal Information Security Modernization Act of 2014 (FISMA). Failure to follow prescribed rules or misuse of federal information and information systems can lead to criminal penalties, including fines and imprisonment, and disciplinary actions according to the contract and/or agreement under which I am performing work for SSA.

I understand that SSA maintains a variety of sensitive information about the agency's operations and programs, which may be information pertaining to program (e.g., information about SSA's clients) or non-program (e.g., administrative and personnel records) matters. I understand that SSA may authorize me to have access to federal information and information systems and that my access to and use of such information and information systems must be in accordance with the provisions of the contract and/or agreement under which I am performing work for SSA.

I understand that the terms in the contract and/or agreement under which I am performing work for SSA take precedence over this document. I understand that any questions I may have concerning authorization(s) to access SSA information and information systems should be directed in accordance with the terms of the contract and/or agreement. I have read, understand, and agree to the following conditions:

Insider Threat

An insider threat is someone with authorized access who uses that access, intentionally or unintentionally, to harm the security of the Agency or the Nation. The individual with authorized access may attempt to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities.

- If I observe a potential insider threat, **I will** report the incident to SSAITP@ssa.gov and, as appropriate, in accordance with the personally identifiable information and incident reporting requirements in the contract or agreement under which I am working.
- **I will** safeguard federal information and information systems from exploitation, compromise, espionage, terrorism, or other unauthorized use and disclosure.

Malware, Remote Access, and Mobile Device Security

Malware encompasses malicious software, programs, files, and/or code in the form of virus, ransomware, and spyware that cause damage to information systems and data. SSA defends against malware using antivirus programs, intrusion detection systems, and social engineering training among other methods. Routine software and security updates ensure SSA devices are up to date with the latest malware protection.

When I have been granted an SSA device to perform work for the agency, the following requirements apply:

- In order to ensure my SSA device receives the necessary software and security updates**, I will** remain connected to SSANet using the agency's Virtual Private Network throughout my workday**, I will** keep my workstation plugged in and powered on, and **I will** restart my workstation at least once a week and at the end of each workday, logging off from the CTRL+ALT+DELETE screen unless further guidance is issued.

- **I will not** store federal information on personally owned media devices or, connect non-SSA approved and issued personal Bluetooth devices to an SSA device.

- **I will not** alter SSA devices, disable security settings, or download or install unauthorized software onto SSA devices.

- **I will** follow the security and safety requirements of any alternative worksite agreement and all contract or agreements related to non-SSA worksites.

- **I will not** print any material that contains federal information at an unapproved location. **I will** protect SSA devices at all times, to include while on travel, at any alternative worksite, and any approved non-SSA worksite.

Secure Browsing and Social Media

Attackers use social data mining techniques to gather information about an individual or organization in public or social settings, including social media. SSA social media accounts are not official SSA websites, but rather the department's presence on third-party service providers' platforms, which means SSA has limited control over how each platform uses personal data provided by users.

- **I will not** transmit, store, or process federal information on non-SSA owned and operated sites, including social media, third party online forums, third-party collaboration tools or sites, social networking sites, any other non-SSA-hosted sites, or unapproved third-party data storage providers unless explicitly authorized to do so.

- **I will not** share programming code used for federal information systems with unauthorized individuals including but not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

- **I will not** use federal information systems to browse or access information about myself, my children, other family members, co-workers or former co-workers, acquaintances, and/or friends.

Secure Email and Fax Use

Email is an official business communication tool and users must use it in a responsible, secure, and lawful manner. When using SSA email, to protect agency systems and those who receive email from me:

- **I will** use business communication tools including SSA email in a responsible, secure, and lawful manner.
- **I will not** send or forward Personally Identifiable Information (PII) to or from a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List.
- **I will not** copy or blind copy work-related email to a personal, non-SSA email address.
- **I will not** send or forward chain letters or other unauthorized mass mailings.
- **I will not** configure my SSA email account to automatically forward work-related email to an outside (non-SSA, non-secure) address.
- If I receive an email intended for someone else, **I will** immediately notify the sender and delete or destroy the misdirected message.

A fax is an official business communication tool and users must use it in a responsible, secure, and lawful manner. When using an SSA fax, to protect agency systems and those who receive faxes from me:

- **I will** use business communication tools including SSA fax in a responsible, secure, and lawful manner.
- **I will** use a cover sheet that notes the sensitivity of the material and follow all Controlled Unclassified Information (CUI) labeling requirements.
- **I will not** leave fax machines unattended when transmitting.
- **I will** transmit faxes to the intended recipient, when possible, using pre-programmed fax numbers.
- **I will not** use SSA's fax system to create or distribute disruptive or offensive messages.
- If I receive a fax by mistake, **I will** notify the sender. To the extent possible, **I will not** read the fax's contents. **I will** destroy the misdirected message.

Security Incident Reporting

Security incidents involve any attempted or actual authorized access, use, disclosure, modification, or destruction of information. Examples include malicious or unauthorized intrusion or access, virus attacks, phishing, vishing, supply chain threats, foreign intelligence threats, insider threats, and loss of PII.

- If I suspect or confirm the loss or theft of any sensitive information, including PII, **I will** report it within one hour to my supervisor, manager, contracting officer's representative and/or contracting officer's technical representative or another designated official. If those individuals are not available, **I will** use the PII Loss Reporting Tool to report any loss or theft of any sensitive information or PII.
- If I observe a suspected systems intrusion attempt or other security-related incident, **I will** report the incident within 15 minutes of discovery to SOC@ssa.gov.
- If I am the targeted victim of a phishing (suspicious email) attempt, **I will** report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- If I am the target of a vishing (suspicious phone call) attempt, **I will** report the incident within 15 minutes of discovery to SOC@ssa.gov.
- If I observe a potential insider threat, **I will** report the incident to SSAITP@ssa.gov. If I observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, **I will** report the incident to the Office of the Inspector General in accordance with published policy.

Social Engineering

Vishing is the practice of tricking you, over the phone, into revealing information to an unauthorized individual or performing actions on your workstation that may compromise the security of SSA.

- **I will** avoid vishing attempts by validating a caller's identity and purpose.
- If I am unable to validate the caller's identity, **I will** hang up and call back using a number I know to be correct.

Phishing is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.

- **I will** avoid phishing attempts by verifying the email sender.
- **I will** be suspicious when receiving emails from individuals I do not know or have not heard from in a long time.
- **I will** never respond to requests for PII or send password information in an email.
- **I will** only release information if I am confident of an individual's identity and right to receive it.

Unauthorized Access and Prohibited Behavior

Unauthorized access to federal information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Federal information system users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time, including accessing the Internet using E-mail.

- **I will not** inspect, access, or attempt to access any federal information that SSA has not expressly authorized me to access.
- **I will not** release or disclose any federal information to any unauthorized person, agency, or entity. **I understand** that unauthorized disclosure of federal information may lead to civil penalties and/or criminal prosecution under Federal law (e.g., The Privacy Act of 1974, 5 U.S.C. 552a; SSA's regulations at 20 C.F.R. Part 401; The Social Security Act, 42 U.S.C. 1306 (a); and 5 U.S.C. Section 552(i)). **I further understand** that additional privacy and disclosure protections may apply to certain types of SSA information including Federal Tax Information (i.e., earnings information), which may be subject to additional penalties under sections 6103, 7213, 7213A, and 7431 of the Internal Revenue Service (IRS) Code (Title 26 of the United States Code).
- **I will** follow all access, retention, and/or destruction requirements in the contract and/or agreement under which I am authorized to access federal information. **I understand** that such requirements may require me to cease access to, return, or destroy federal information upon completion of my work for SSA or termination of my contract and/or agreement that authorized my access to federal information.
- **I will not** take federal information off-site, unless expressly authorized to do so by contract and/or agreement or other written authorization from SSA. If SSA authorizes me to take federal information off-site, I agree to safeguard all such information in accordance with agency policy and standards and the requirements of the contract and/or agreement under which I am performing work so that no unauthorized person, agency, or entity can access federal information.
- **I will** keep confidential any third-party proprietary information that may be entrusted to me as part of the contract and/or agreement, including safeguarding such information from unauthorized access and not disclosing or releasing such information unless expressly authorized to do so.
- **I will** follow all requirements in the contract and/or agreement under which I am performing work for SSA, includingbut not limited to those governing confidential information or PII.
- **I will** only use my access to federal information and information systems for the performance of my official duties.

Contractor Employee Name (Print/Type)	Date (MM/DD/YYYY)
Contractor Employee Signature (Sign)	

Contract Number	Company Name (Print/Type)
Company Point Of Contact (Print/Type)	Company Point of Contact Phone Number

Privacy Act
Collection and Use of Personal Information

42 U.S.C. § 904(a); 20 C.F.R. § 401.90; 44 U.S.C. §§ 3541-3549; 41 C.F.R. Chapter 101; 5 U.S.C. § 552a(e)(9)-(10); and Executive Order 13488 of the Social Security Act, as amended, allow us to collect this information. Furnishing this information to the Social Security Administration (SSA) is voluntary. However, failing to provide this information may affect your ability to access Federal information and information systems, which is a condition of the contract under which you are performing work for SSA (SSA contract). Not providing this information also could prevent us from issuing you a PIV credential and/or authorizing you to access SSA's network, one or both of which may be conditions of your SSA contract. Failure to follow prescribed rules or misuse of SSA information and information systems could lead to removal from duty from your SSA contract.

We will use the information you provide to grant you access to Federal information and information systems. We may also share your information for the following purposes, called routine uses:

- To contractors and other Federal agencies, as necessary, for assisting SSA in the efficient administration of its programs. We disclose information under this routine use only in situations in which SSA may enter into a contractual or similar agreement with a third party to assist the accomplishing an agency function relating to this system of records; and

- To student volunteers, individuals working under a personal services contract, and other workers who individuals performing functions for SSA but technically do not having the status of Federal agency employees, when they are performing work for SSA, as authorized by law, and if they need access to personally identifiable information (PII) in SSA the records in order to perform their assigned agency functions.

In addition, we may share this information in accordance with the Privacy Act and other Federal laws. For example, where authorized, we may use and disclose this information in computer matching programs, in which our records are compared with other records to establish or verify a person's eligibility for Federal benefit programs and for repayment of incorrect or delinquent debts under these programs.

A list of additional routine uses is available in our Privacy Act System of Records Notice (SORN) 60-0361, entitled Identity Management System, as published in the Federal Register (FR) on November 3, 2006, at 71 FR 64751. Additional information, and a full listing of all our SORNs, is available on our website at www.ssa.gov/privacy.

EXHIBIT H

Sample Stock Replenishment Task Order / Sample Task Order

	A	B	C	D	E	F	G
1	Task_Order	Replenishment_Number	Product_ID	Edition_Date	Product_Type	Replenishment_Type	Quantity
2	99-99999-9	99-99126	552500		O	Receive	1000
3	99-99999-9	REPL-FY-#####	05-10550	01/2020 or 03/2018	P	Print	5000
4	99-99999-9	REPL-FY-#####	SS-5	02/2020	F	Print	150000
5	99-99999-9	PPREQ-FY-#####	ENV-00025		E	Receive	200000

Sample Stock Replenishment Task Order / Sample Task Order

	H	I	J	K
1	Unit_of_Issue	Submitted_By	Finish_Date	Cancel_Item
2	Each	kathryn.schmidt@ssa.gov	5/1/2020	Cancel
3	Package of 100	kathryn.schmidt@ssa.gov	5/5/2020	
4	Package of 100	kathryn.schmidt@ssa.gov	5/5/2020	
5	Case of 500	kathryn.schmidt@ssa.gov	5/15/2020	

Sample Stock Replenishment Task Order / Task Order Data Spec

	A	B	C	D	E
1	Task_Order	Replenishment_Num	Product_ID	Edition_Date	Product_Type
2	Task Order the Replenishment was part of	The Replenishment number assigned to that items replenishment request	Product ID being replenished	The authorized edition date for the Product ID being replenished.	P = Publication F = Form E = Envelope O = Other

Sample Stock Replenishment Task Order / Task Order Data Spec

	F	G	H	I	J	K
1	Replenishment_Typ	Quantity	Unit_of_Issue	Submitted_By	Finish_Date	Cancel_Item
2	Print = Print Replenishment Receive = Receiving Replenishment	Quantity Requested for Replenishment	Unit of issue the producdt will be stocked in	Email address of the SSA analyst that submitted the order.	Date this item will be received or must be printed and stocked by.	The word "Cancel" will display if the item replenishment is being cancelled. This is only valid for items that will be received. Printed items will be cancelled via direct contact with the SSA analyst.

EXHIBIT I

Sample Fulfillment Task Order / Sample Task Order

	A	B	C	D	E	F	G	H
1	Print_Order	Task_Order	Order_Number	Product_ID	Edition_Date	Product_Type	Quantity	Foreign_Domestic
2	99-99999	99-99999-9	99-99126	552500		O	25	D
3	99-99999	99-99999-9	99-99126	05-10550	01/2020 or 03/2018	P	25	D
4	99-99999	99-99999-9	99-99126	SS-5	02/2020	F	5000	D
5	99-99999	99-99999-9	99-99126	ENV-00025		E	500	D

Sample Fulfillment Task Order / Sample Task Order

	I	J	K
1	Office_Name	Address_Line1	Address_Line2
2	***** TEST - TEST - TEST *****	***** TEST - TEST - TEST *****	***** TEST - TEST - TEST *****
3	***** TEST - TEST - TEST *****	***** TEST - TEST - TEST *****	***** TEST - TEST - TEST *****
4	***** TEST - TEST - TEST *****	***** TEST - TEST - TEST *****	***** TEST - TEST - TEST *****
5	***** TEST - TEST - TEST *****	***** TEST - TEST - TEST *****	***** TEST - TEST - TEST *****

Sample Fulfillment Task Order / Sample Task Order

	L	M	N	O	P	Q
1	Address_Line3	Address_Line4	City	State	Zip	Plus_4
2	***** TEST - TEST - TEST *****	***** TEST - TEST - TEST *****	SOMERSET	??	42501	9801
3	***** TEST - TEST - TEST *****	***** TEST - TEST - TEST *****	SOMERSET	KY	42501	9801
4	***** TEST - TEST - TEST *****	***** TEST - TEST - TEST *****	SOMERSET	KY	42501	9801
5	***** TEST - TEST - TEST *****	***** TEST - TEST - TEST *****	SOMERSET	KY	42501	9801

Sample Fulfillment Task Order / Sample Task Order

	R	S	T	U
1	Postal_Code	Country_Name	Cancel_Item	
2			Cancel	
3				
4				
5				

Sample Fulfillment Task Order / Task Order Data Spec

	A	B	C	D	E	F
1	Print_Order	Task_Order	Order_Number	Product_ID	Edition_Date	Product_Type
2	Print Order Number Standard format as shown on the sample.	Task Order Number Standard format as shown on the sample.	MyStock Order Number Standard format as shown on the sample.	Product ID	Edition Date to be fulfilled. If an "or" statement then either of the shown edition dates may be fulfilled for the order.	P = Publication F = Form E = Envelope O = Other

	G	H	I	J	K	L	M	N	O	P
1	Quantity	Foreign_Domestic	Office_Name	Address_L	Address_L	Address_L	Address_L	City	State	Zip
2	Quantity to fulfill.	D = Domestic F = Foreign	Columns I - S are shipping address information to be used for the fulfillment							

	Q	R	S	T
1	Plus_4	Postal_Co	Country_N	Cancel_Item
2				The word "Cancel" will appear when a customer has requested to cancel an item from their order. This will only appear for items that were part of a previous task order.

EXHIBIT J

Initial Stock Retrieval Report / Sample Retrieving Report

	A	B	C	D	E	F
1	Product_ID	Edition_Date	Product_Type	Quantity	Current_Unit_of_Issue	Repackage_Unit_of_Issue
2	552500		O	1000	Each	
3	05-10550	01/2020	P	5000	Package of 100	Package of 25
4	SS-5	02/2020	F	150000	Package of 100	Package of 25
5	ENV-00025		E	200000	Case of 500	

Initial Stock Retrieval Report / Data Spec

	A	B	C	D	E
1	Product_ID	Edition_Date	Product_Type	Quantity	Current_Unit_of_Issue
2	Product ID of the item being retrieved	Edition date of the product being retrieved	P = Publication F = Form E = Envelope O = Other	Quantity being retrieved	This is the unit of issue that the item is currently packaged in when retrieved.
3					

Initial Stock Retrieval Report / Data Spec

	F
1	Repackage_Unit_of_Issue
2	This is the unit of issue the contractor will repackage the product after retrieval.
3	If this is blank then the product will not need to be repackaged

EXHIBIT K

Inventory Update File Template / Sample Inventory Status Update

	A	B	C	D
1	Product_ID	Edition_Date	Product_Type	Quantity
2	05-11015	01/2020	P	5000
3	05-10550	03/2018	P	50
4	05-10540	01/2020	P	-250
5	05-10531	01/2020	P	100000
6	05-10530	07/2019	P	22525
7	05-10525	05/2016 and 02/2020	P	875

Inventory Update File Template / Inventory Update Data Spec

	A	B	C	D
1	Product_ID	Edition_Date	Product_Type	Quantity
2	Product ID	Edition Date in stock. If multiple editions are stocked the edition dates will be seperated by the word "and". Only Approved Edition Dates should ever be stocked.	P = Publication F = Form E = Envelope O = Other	Quantity in stock. If Back Orders exist for an item then the volume will display as a negative.

EXHIBIT L

Replenishment Status Update File Template / Sample Task Order

	A	B	C	D	E	F	G
1	Task_Order	Replenishment_Number	Product_ID	Edition_Date	Product_Type	Replenishment_	Quantity
2	99-99999-9	99-99126	552500		O	Receive	
3	99-99999-9	99-99126	05-10550	01/2020	P	Print	1000
4	99-99999-9	99-99126	SS-5	02/2020	F	Print	150000
5	99-99999-9	99-99126	ENV-00025		E	Receive	200000

Replenishment Status Update File Template / Sample Task Order

	H	I	J
1	Unit_of_Issue	Date_Completed	Cancel_Item
2	Each	5/1/2020	C
3	Package of 100	5/5/2020	P
4	Package of 100	5/5/2020	
5	Case of 500	5/15/2020	

Replenishment Status Update File Template / Task Order Data Spec

	A	B	C	D	E
1	Task_Order	Replenishment_Number	Product_ID	Edition_Date	Product_Type
2	Task Order Number Standard format as shown on the sample.	The Replenishment Number	Product ID that was replenished.	The edition date replenished for the Product ID.	P = Publication F = Form E = Envelope O = Other
3					

Replenishment Status Update File Template / Task Order Data Spec

	F	G	H	I	J
1	Replenishment_Type	Quantity	Unit_of_Issue	Date_Completed	Cancel_Item
2	Print = Print Replenishment Receive = Receiving Replenishment	Quantity printed or received.	The unit of issue the item is packaged in	The date this replenishment was completed.	"C" if item was completely cancelled. "P" if item was only partially cancelled.
3		This field is not mandatory if the "Cancel_Item" field is "C"			

EXHIBIT M

Fulfillment Status Update File Template / Sample

	A	B	C	D	E	F	G
1	Order_Number	Product_ID	Edition_Date	Quantity	Shipping Status	Date_Shipped	Shipping_Method_ID
2	19-05449	SS-5	02/2020	250	S	12/5/2018	2
3	19-05449	SS-5	02/2020	250	S	12/5/2018	2
4	19-05450	05-10552	01/2019	250	S	12/5/2018	2
5	19-05450	05-10540	05/2016	200	S	12/5/2018	2
6	19-05450	05-10511	01/2020	100	S	12/5/2018	2
7	19-05450	05-10056	07/2018	200	S	12/5/2018	2
8	19-05451	SS-5-SP		100	B		
9	19-05451	SS-5		250	C		
10	19-05451	SS-5	02/2021	250	S	12/5/2018	2
11	19-05452	SS-5	02/2022	250	S	12/5/2018	2
12	19-05452	SS-5	02/2023	250	S	12/5/2018	2
13	19-05453	05-10153	01/2019	200	B		
14	19-05453	05-10069	05/2016	200	S	12/5/2018	2
15	19-05454	05-10540	01/2020	25	S	12/5/2018	2
16	19-05455	70-10281	01/2019	25	S	12/5/2018	2
17	19-05455	05-10095	05/2016	25	S	12/5/2018	2
18	19-05455	05-10090	01/2020	25	S	12/5/2018	2
19	19-05455	05-10087	01/2020	25	B		

Fulfillment Status Update File Template / Sample

	H	I	J
1	Shipping_Method_Code	Tracking_Number	
2	UPS	1Z2VR1810343211116	
3	UPS	1Z2VR1810343211117	
4	UPS	1Z2VR1810343211126	
5	UPS	1Z2VR1810343211126	
6	UPS	1Z2VR1810343211118	
7	UPS	1Z2VR1810343211120	
8			
9			
10	UPS	1Z2VR1810343211123	
11	UPS	1Z2VR1810343184102	
12	UPS	1Z2VR1810343184103	
13			
14	UPS	1Z2VR1810343211129	
15	UPS	1Z2VR1810343184130	
16	UPS	1Z2VR1810343211144	
17	UPS	1Z2VR1810343211144	
18	UPS	1Z2VR1810343211144	
19			

Fulfillment Status Update File Template / Data Spec

	A	B	C	D
1	Order_Number	Product_ID	Edition_Date	Quantity
2	MyStock Order Number	Product ID that was fulfilled	Edition Date of the Product ID fulfilled	Quantity Fulfilled
3				Blank if "Shipping_Status" = C or B

Fulfillment Status Update File Template / Data Spec

	E	F	G	H
1	Shipping Status	Date_Shipped	Shipping_Method_ID	Shipping_Method_Code
2	S = Shipped B = Back Order C = Cancelled	Date Item was shipped	1 = USPS 2 = UPS	If Shipping_Method_ID is 1 then "USPS" If "Shipping_Method_ID" is 2 then "UPS"
3		Blank if "Shipping_Status" = C or B	Blank if "Shipping_Status" = C or B	Blank if "Shipping_Status" = C or B

Fulfillment Status Update File Template / Data Spec

	I
1	Tracking_Number
2	Tracking number if sent via SPCC. Mandatory If Shipping_Method = "2"
3	Blank if "Shipping_Status" = C or B

EXHIBIT N

Printed Items Specification data table / Printed Form Products

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Form Number	Format	Form Title	Number of text pages	Prints	Flat Size: Width	Flat Size: Height	Finished Size: Width	Finished Size: Height	Fold to Size: Width	Fold to Size: Height	Margins: Face Left	Margins: Face Top	Margins: Back Right
2	HA-501-U5	Format G	Request For Hearing By Administrative Law Judge	10	Head to Head	8.5	11					1/4	5/8	1/4
3	HA-501-U5-SP	Format G	Request For Hearing by Administrative Law Judge	2	Head to Head	8.5	11					1/4	5/8	1/4
4	HA-520-U5	Format G	Request For Review Of Hearing Decision/Order	5	Head to Head	8.5	11					3/4	1 1/2	1 3/4
5	HA-520-U5-SP	Format G	Request For Review Of Hearing Decision/Order	10	Head to Head	8.5	11					3/4	0.5	1.25
6	SS-5	Format D	Application For A Social Security Card	5	Head to Head	25.5	11			8.5	3.75	1/4	1/4	1/4
7	SS-5-FS	Format D	Application For A Social Security Card	5	Head to Head	25.5	11	8.5	11	8.5	3.75	1/4	1/4	1/4
8	SS-5-SP	Format D	Application For A Social Security Card - Spanish	5	Head to Head	25.5	11			8.5	3.66			
9	SSA-1020-B-OCR-SM	Format C	Application For Help With Medicare Prescription Drug Plan Costs Notice/Scannable Form	8	Head to Head	17	11	8.5	11			1/4	1/4	1/4
10	SSA-1020-B-OCR-SM-SP	Format C	Application For Help With Medicare Prescription Drug Plan Costs Notice / Scannable Form Spanish	8	Head to Head	17	11	8.5	11			1/4	1/4	1/4
11	SSA-1026-B-OCR-SM	Format C	Review of your Eligibility for Extra Help with Medicare Prescription Drug Plan Costs Summary Notice and Scannable Form	8	Head to Head	17	11	8.5	11			1/4	1/4	1/4
12	SSA-1026-B-OCR-SM-SP	Format C	Review of your Eligibility for Extra Help with Medicare Prescription Drug Plan Costs Summary Notice and Scannable Form Spanish	8	Head to Head	17	11	8.5	11			1/4	1/4	1/4
13	SSA-1054	Format A	Hearing Case Expedite Cards	1	One Side	5	3							
14	SSA-1128	Format A	Representative Involved	1	One Side	5	3					1/4	3/16	

Printed Items Specification data table / Printed Form Products

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Form Number	Format	Form Title	Number of text pages	Prints	Flat Size: Width	Flat Size: Height	Finished Size: Width	Finished Size: Height	Fold to Size: Width	Fold to Size: Height	Margins: Face Left	Margins: Face Top	Margins: Back Right
15	SSA-117-PC	Format B	Customer Comment Card	2	Head to Head,Head to Side	11	8.5			5.5	8.5	1/4	1/4	1/4
16	SSA-117-PC-SP	Format B	Customer Comment Card - Spanish	4	Head to Head	11	8.5			5.5	8.5			
17	SSA-11-BK	Format E	Request To Be Selected As Payee	10	Head to Head	17	11	8.5	11			5/8	1/2	5/8
18	SSA-124-U3	Format G	Remittance Register Pre Number	1	One Side	16	10.5					1		
19	SSA-1395-BK	Format E	Receipt And Transmittal Form	6	Head to Head	25 7/8	3.25	7 3/8	3 1/4	7 3/8	3 1/4			
20	SSA-16	Format C	Application For Disability Insurance Benefits	8	Head to Head	17	11	8.5	11	8.5	11	5/8	1/4	5/8
21	SSA-1690	Format A	Transmittal Of Material To The Public	1	One Side	8.5	3.75							
22	SSA-1719-B	Format C	SSI Posteligibility Data Input	2	Head to Head	17	11	8.5	11	8.5	11	3/4	1/4	3/4
23	SSA-1719-C	Format B	Supplemental Security Income Posteligibility Input-Short Form	2	Head to Head	11	8.5					1	1	1.25
24	SSA-1719-DM	Format C	Supplemental Security Income Posteligibility Data Input--Debt Collection Processing	1	One Side	14	8.5							
25	SSA-1994	Format B	Cover Sheet Confidential Medical Information	1	One Side	8.5	11					1/2	1/4	
26	SSA-2204	Format B	Payment Worksheet - Self	2	Head to Head	11	8.5					1/2	5/16	1/2
27	SSA-2458	Format B	Report Of Confidential Social Security Benefit Information	1	One Side	8.5	11					1/2	1/2	
28	SSA-2708	Format B	Field Office Call/Come In Request	1	One Side	8.5	11					1/2	1/4	
29	SSA-2848	Format B	Quality Assurance Review Sample Case	1	One Side	8.5	11					Center	Center	
30	SSA-2853	Format B	Message From Social Security- 5 Weeks	1	One Side	11	8.5					0.5	0.5	
31	SSA-2853-OP1	Format B	Message From Social Security - 4 Weeks	1	One Side	11	8.5							
32	SSA-2853-OP1-SP	Format B	Message From Social Security- 4 Weeks (Spanish)											
33	SSA-2853-OP2	Format B	Message From Social Security - 3 Weeks	1	One Side	11	8.5					.5	.5	

Printed Items Specification data table / Printed Form Products

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Form Number	Format	Form Title	Number of text pages	Prints	Flat Size: Width	Flat Size: Height	Finished Size: Width	Finished Size: Height	Fold to Size: Width	Fold to Size: Height	Margins: Face Left	Margins: Face Top	Margins: Back Right
34	SSA-2853-OP2-SP	Format B	Message From Social Security - 3 Weeks (Spanish)	1	One Side	11	8.5					.5	.5	
35	SSA-2853-OP3	Format B	Message From Social Security - 6 Weeks	1	One Side	11	8.5					1/2	1/2	
36	SSA-2853-OP4	Format B	Message From Social Security - 10 Weeks	1	One Side	11	8.5					1/2	1/2	
37	SSA-2853-OP4-SP	Format B	Message From Social Security - 10 Weeks (Spanish)	1	One Side	11	8.5					1/2	1/2	
38	SSA-2900	Format B	Participant Name Card	1	One Side	11	8.5					Center	Center	
39	SSA-3105	Format B	Important Information About Your Appeal, Waiver Rights, and Repayment Options	2	Head to Head	10.5	8	3.5	8					
40	SSA-3288	Format B	Social Security Administration Consent For Release Of Information	2	Head to Head	8.5	11					1/4	1/4	1/4
41	SSA-3368-BK	Format E	Disability Report - Adult	14	Head to Head	17	11			8.5	11	5/8	1/4	5/8
42	SSA-3369-BK	Format E	Work History Report	10	Head to Head	17	11			8.5	11	5/8	5/8	5/8
43	SSA-3371-BK	Format E	Pain Report - Child	12	Head to Head	17	11			8.5	11	1/4	1/4	1/4
44	SSA-3373-BK	Format E	Function Report - Adult	10	Head to Head	17	11			8.5	11	5/8	1/4	5/8
45	SSA-3375-BK	Format E	Function Report - Child (Birth to 1st Birthday)	7	Head to Head	17	11			8.5	11	5/8	1/2	5/8
46	SSA-3376-BK	Format E	Function Report - Child (Age 1 To 3rd Birthday)	9	Head to Head	17	11	8.5	11					
47	SSA-3377-BK	Format E	Function Report - Child (Age 3 To 6th Birthday)	10	Head to Head	17	11			8.5	11			
48	SSA-3378-BK	Format E	Function Report - Child (Age 6 To 12th Birthday)	12	Head to Head	17	11			8.5	11			
49	SSA-3379-BK	Format E	Function Report - Child (Age 12 To 18th Birthday)	11	Head to Head	17	11			8.5	11	5/8	1/2	5/8
50	SSA-3380-BK	Format E	Function Report Adult Third Party Booklet	10	Head to Head	17	11	8.5	11	8.5	11			
51	SSA-3441-BK	Format E	Disability Report-Appeal	10	Head to Head	17	11			8.5	11	3/4	1/2	3/4
52	SSA-3441-BK-SP	Format E	Disability Report-Appeal (Spanish)	10	Head to Head	17	11	8.5	11	8.5	11	1/2	3/4	1/2

Printed Items Specification data table / Printed Form Products

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Form Number	Format	Form Title	Number of text pages	Prints	Flat Size: Width	Flat Size: Height	Finished Size: Width	Finished Size: Height	Fold to Size: Width	Fold to Size: Height	Margins: Face Left	Margins: Face Top	Margins: Back Right
53	SSA-3601	Format B	Claims Routing	1	One Side	8.5	11							
54	SSA-3820-BK	Format E	Disability Report - Child	14	Head to Head	17	11			8.5	11	5/8	1/4	5/8
55	SSA-3881-BK	Format E	Questionnaire For Children Claiming SSI Benefits	8	Head to Head	17	11			8.5	11	5/8	1/2	5/8
56	SSA-4074	Format B	Rec Of Time Of Arrival And Dep	2	Head to	11	8.5					5/16	5/8	5/16
57	SSA-408	Format A	Route Slip	1	One Side	4.25	5.5							
58	SSA-409	Format B	Postadjudicative Routing	1	One Side	8.5	11					1/2	1/4	
59	SSA-4111	Format B	Certificate Of Election For Reduced Widow(er)'s And Surviving Divorced Spouse's Benefits	2	Head to Head	8.5	11					1/4	5/16	1/2
60	SSA-4290-F5	Format D	Development Of Participation In Vocational Rehabilitation or Similar Program	5	Head to Head	25.5	11	8.5	11	8.5	11			
61	SSA-445	Format B	Application To Collect A Fee For Payee Services	2	Head to Head	8.5	11							
62	SSA-450-SI	Format C	SSI Data Input And Determination	1	One Side	17	11			8.5	11	3/4	1/4	3/4
63	SSA-453-F4	Format C	How Your Earnings Affect Your Benefits	4	Head to Head	17	11	8.5	11	8.5	11	1/2	1/4	1/2
64	SSA-454-BK	Format E	Continuing Disability Review Report	15	Head to Head	17	11			8.5	11	5/8	1/4	5/8
65	SSA-4904-U2	Format G	Supplemental Security Income Monthly Payment Computation Summary	2	One Side	8.5	11					1/2	5/8	
66	SSA-4-BK	Format E	Application For Child's Insurance Benefits	9	Head to Head	17	11			8.5	11	5/8	5/8	1/4
67	SSA-5002	Format B	Report Of Contact	1	One Side	8.5	11					3/4	1/2	
68	SSA-5028	Format A	Receipt For Application For A SSN	1	One Side	8	5 1/4					1	1/2	
69	SSA-533	Format B	Translation Request	2	Head to Head	8.5	11					5/8	1/4	5/8
70	SSA-544	Format B	Exhibits Marker	1	One Side	8.5	11					3/4	1/2	
71	SSA-545-BK	Format E	PLAN TO ACHIEVE SELF-SUPPORT (PASS)	12	Head to Head	17	11	8.5	11	8.5	11	0.5	0.25	0.5
72	SSA-559	Format A	Transmittal Slip For Claims Folder	1	One Side	5.5	8.5					1/4	5/16	
73	SSA-561-U2	Format G	Request For Reconsideration	4	Head to Head	8.5	11					5/8"	1/4"	5/8"
74	SSA-6029-C6	Format G	Receiving Report	6	One Side									
75	SSA-6234-F6	Format D	Representative Payee Report	6	Head to Head	25.5	11	8.5	11	8.5	11			

Printed Items Specification data table / Printed Form Products

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Form Number	Format	Form Title	Number of text pages	Prints	Flat Size: Width	Flat Size: Height	Finished Size: Width	Finished Size: Height	Fold to Size: Width	Fold to Size: Height	Margins: Face Left	Margins: Face Top	Margins: Back Right
76	SSA-624-F5	Format D	Representative Payee Evaluation Report	5	Head to Head	25.5	11			8.5	11			
77	SSA-632-BK-SP	Format E	Request for Waiver Of Overpayment Recovery - Spanish	9	Head to Head	17	11	8.5	11	8.5	11	5/8	1/4	5/8
78	SSA-636	Format A	Transmittal Notice Hearing Case	1	One Side			5.25	8			3/4	1/4	
79	SSA-7050-F4	Format C	Request For Social Security Earnings Information	4	Head to Head	17	11			8.5	11	5/8	1/2	5/8
80	SSA-708	Format A	Work Lot Record Card	1	One Side			7 3/8	3 1/4			1/4	5/16	
81	SSA-71	Format B	Application For Leave	2	Head to Head	7 1/4	10 1/4					3/16	3/16	3/16
82	SSA-714	Format B	You Can Make Your Payment By Credit Card	1	One Side	8.5	11							
83	SSA-721	Format C	Statement Of Death By Funeral Director	3	Head to Head	17	11			8.5	11	3/4	3/8	1
84	SSA-787	Format C	Physician's/Medical Officer's Statement Of Patient	4	Head to Head	17	11			8.5	11	5/8	1/4	5/8
85	SSA-795	Format B	Statement Of Claimant Or Other Person	2	Head to Head	8.5	11					5/8	1/4	3/4
86	SSA-8	Format D	Application For Lump Sum Death Payment	4	Head to Head	25.5	11	8.5	11			5/8	1/4	5/8
87	SSA-8000-BK	Format E	Application For Supplemental Security Income	24	Head to Head	17	11			8.5	11			
88	SSA-8001-BK	Format E	Application For SSI	12	Head to Head	17	11			8.5	11	5/8	1/4	5/8
89	SSA-8006-F4	Format C	Stmt Of Living Arrangements	4	Head to Head	17	11	8.5	11			5/8	1/4	5/8
90	SSA-8008	Format B	Living Arrangement Development	2	Head to Head	8.5	11					1/4	1/4	1/4
91	SSA-8010-BK	Format E	Statement Of Income And Resources	12	Head to Head	17	11			8.5	11	5/8	1/4	5/8
92	SSA-8203-BK	Format E	Statement For Determining Continuing Eligibilty For Supplemental Security Income Payments	10	Head to Head	17	11			8.5	11	5/8	1/4	5/8

Printed Items Specification data table / Printed Form Products

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Form Number	Format	Form Title	Number of text pages	Prints	Flat Size: Width	Flat Size: Height	Finished Size: Width	Finished Size: Height	Fold to Size: Width	Fold to Size: Height	Margins: Face Left	Margins: Face Top	Margins: Back Right
93	SSA-8240	Format C	AUTHORIZATION FOR THE SOCIAL SECURITY ADMINISTRATION TO OBTAIN WAGE AND EMPLOYMENT INFORMATION FROM PAYROLL DATA PROVIDERS	3	Head to Head	17	11			8.5	3.66	1/4	1/4	1/4
94	SSA-827	Format B	Authorization To Disclose Information To The Social Security Administration	2	Head to Head	8.5	11					5/8	1/4	5/8
95	SSA-827-F3	Format B	Authorization to Disclose Information to the Social Security Administration	2	Head to Head	8.5	11	8.5	3 2/3	8 1/2	3 2/3	1/4	1/4	1/4
96	SSA-8-SP	Format D	Application For Lump Sum Death Payment	4	Head to Head	25.5	11	8.5	11			1/4	1/4	1/4
97	SSA-961-U3	Format G	Urgent Folder Request	1	One Side	8.5	11					5/8		
98	SSA-L1013	Format B	Social Security Notice Of Continued Disability	2	Head to Head	8.5	11					1	2 3/16	3/4
99	SSA-L2880	Format B	Social Security Number Evidence Return Notice	1	One Side	8.5	11							
100	SSA-L4201-BK	Format E	Letter To Employer Requesting Wage Information	6	Head to Head	17	11			8.5	11	1/2	1/2	1/2
101	SSA-L634	Format B	Social Security Benefit Information	1	One Side	8.5	11					1	1/2	
102	SSA-L725-F3	Format C	Employer Requesting Report	3	Head to Head	17	11	8.5	11			3/4	3/4	3/4

Printed Items Specification data table / Printed Form Products

	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF
1	Margins: Back Top	Paper: Color	Paper: Weight	Paper: Type	Paper: Ink	Multipart form	Drilling: Number of holes	Drilling: Position	Drilling: Diameter	Drilling: Inches center to center	Drilling: Inches from edge	Padding: Position	Padding: Sets must register	Padding: Chipboard Required	Padding: Sheets per pad	Padding: Sets per pad	Padding: Sheets per set	Finishing: Perforation
2	5/8	Multi			Black	Yes	2	Left	9/32	2 3/4	3/8	Top	Yes	No	10	5	2	No
3	5/8				Black	Yes	2	Left	9/32	2 3/4	3/8	Top	Yes	No	10	5	2	No
4	1 1/2	Multi		NCR	Black	Yes	2	Left	1/4	2 3/4	3/8	Top	Yes	No	5			No
5	1	Multi		NCR	Black	Yes	2	Left	1/4	2 3/4	3/8	Top	No					
6	1/4	White	20 lb	CW Writing	Black	No							No	No				Yes
7	1/4	White	20 lb	CW Writing	Black	No												Yes
8		White	20 lb	CW Writing	Black	No							No	No				Yes
9	1/4	White	20 lb	Writing	Black	No												
10	1/4	White	20 lb	Writing	Black	No												
11	1/4	White	20 lb	Writing	Black	no												
12	1/4	White	20 lb	Writing	Black	No												
13		Salmon	44 lb	Ledger	Black	no						Top	No	No	50			
14		Blue	44	Ledger	Black	No						Top	No	No	100			No

Printed Items Specification data table / Printed Form Products

	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF
1	Margins: Back Top	Paper: Color	Paper: Weight	Paper: Type	Paper: Ink	Multipart form	Drilling: Number of holes	Drilling: Position	Drilling: Diameter	Drilling: Inches center to center	Drilling: Inches from edge	Padding: Position	Padding: Sets must register	Padding: Chipboard Required	Padding: Sheets per pad	Padding: Sets per pad	Padding: Sheets per set	Finishing: Perforation
15	1/4	White	44 lb	Ledger	Black	No							No	No				Yes
16		White	44	Ledger	Black	No							No	No				Yes
17	1/2	Yellow	20	CW Writing	Black	No							No	No				No
18		Multi		NCR	Black	Yes	2	Left	1/4	2 3/4	3/8	Left	Yes		150	50	3	
19		Multi	Multi	NCR	Black	No							Yes		50	25	2	Yes
20	1/4	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8							Yes
21		White	16 lb	CW Writing	Black	No							No	No				No
22	1/4	White	20 lb	CW Writing	Black	No												
23	1	White	20	CW Writing	Black	No							No	No				No
24		White	20 lb	CW Writing	Black	No												
25		Pink	20 lb	CW Writing	Black	No												
26	5/16	White	20 lb	CW Writing	Black	No												
27		White	20 lb	CW Writing	Black	No							No	No				No
28		White	20 lb	CW Writing	Black	No							No	No				No
29		White	20 lb	CW Writing	Black	No												
30		White	20#	CW	Black	No							No	No				No
31		White	20#	CW Writing	Black	No							No	No				No
32																		
33		White	20 lb	CW Writing	Black	No												

Printed Items Specification data table / Printed Form Products

	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF
1	Margins: Back Top	Paper: Color	Paper: Weight	Paper: Type	Paper: Ink	Multipart form	Drilling: Number of holes	Drilling: Position	Drilling: Diameter	Drilling: Inches center to center	Drilling: Inches from edge	Padding: Position	Padding: Sets must register	Padding: Chipboard Required	Padding: Sheets per pad	Padding: Sets per pad	Padding: Sheets per set	Finishing: Perforation
34		White	20 lb	CW Writing	Black	No												
35		White	20 lb	CW Writing	Black	No												
36		White	20	CW Writing	Black	No							No	No				No
37		White	20 lb	CW Writing	Black	No												
38		White	44 lb	Ledger	PMS 277 c	No												
39		White	20 lb	CW Writing	Black	No												Yes
40	1/4	White	20 lb	CW Writing	Black	No							No	No				No
41	1/4	Green	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
42	1/4"	Buff	20	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
43	1/4	White	20 lb	CW Writing	Black	No							No	No				Yes
44	1/4	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
45	1/2	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
46		White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
47		White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
48		White	20 lb	CW Writing	Black	No	2	Top	9/32	2 3/4	3/8		No	No				Yes
49	1/2	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
50		Blue	20 lb	CW Writing	Black	no	2	Left	9/32	2 3/4	3/8		No	No				Yes
51	1/2	Yellow	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
52	3/4	Yellow	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		no	no				Yes

Printed Items Specification data table / Printed Form Products

	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF
1	Margins: Back Top	Paper: Color	Paper: Weight	Paper: Type	Paper: Ink	Multipart form	Drilling: Number of holes	Drilling: Position	Drilling: Diameter	Drilling: Inches center to center	Drilling: Inches from edge	Padding: Position	Padding: Sets must register	Padding: Chipboard Required	Padding: Sheets per pad	Padding: Sets per pad	Padding: Sheets per set	Finishing: Perforation
53		White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				No
54	1/4	Blue	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
55	1/2	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				No
56	1/2	White	20 lb	CW Writing	Black	No	3	Top										
57		Green	20 lb	CW Writing	Black	No						Top	No	No	100			No
58		Yellow	20 lb	CW Writing	Black	No							No	No				No
59	1/2	White	20 lb	CW Writing	Black	No							No	No				No
60		White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8							
61		White	20 lb	CW Writing	Black	No							No	No				No
62	1/4	White	20 lb	CW Writing	PMS 463 E	No							No	No				No
63	1/4	White	20 lb	CW Writing	Black	No												
64	1/4	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
65		Multi	15 lb	NCR	Black	Yes	2	Top	9/32	2 3/4	3/8	Top	Yes	No	2	1	2	No
66	1/4	Yellow	20	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
67		White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8	Top	No	No	100			No
68		White	16 lb	CW Writing	Black	No						Top	No	No	100			No
69	1/4	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8							
70		Pink	110	Ledger	Black	No	2	Left	9/32	2 3/4	3/8							
71	0.25	Yellow		CW Writing	Black	No							No	No				No
72		White	20	CW Writing	Black	No												
73	1/4'	White	15	NCR	Black	Yes	2	Left	9/32"	2.75"	3/8"	Top	Yes	No			2	No
74																		
75		White	20 lb	CW Writing	Black													

Printed Items Specification data table / Printed Form Products

	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF
1	Margins: Back Top	Paper: Color	Paper: Weight	Paper: Type	Paper: Ink	Multipart form	Drilling: Number of holes	Drilling: Position	Drilling: Diameter	Drilling: Inches center to center	Drilling: Inches from edge	Padding: Position	Padding: Sets must register	Padding: Chipboard Required	Padding: Sheets per pad	Padding: Sets per pad	Padding: Sheets per set	Finishing: Perforation
76		White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
77	1/4	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8							
78		White	20 lb	CW Writing	Black	No						Top	No	No			100	No
79	1/2	White	20 lb	CW Writing	Black	No							No	No				Yes
80		Buff	44 lb	Ledger	Black	No												
81	1/2	White	20 lb	CW Writing	Black	No							No	No				Yes
82		White	20 lb	CW Writing	Black	No												
83	1	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
84	1/4	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
85	1/4	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				No
86	1/4	Buff	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8							
87		White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
88	1/4	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
89	1/4	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8							
90	1/4	White	20 lb	CW Writing	Black	No												
91	1/4	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes
92	1/4	White	20 lb	CW Writing	Black	No	2	Left	9/32	2 3/4	3/8		No	No				Yes

Printed Items Specification data table / Printed Form Products

	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF
1	Margins: Back Top	Paper: Color	Paper: Weight	Paper: Type	Paper: Ink	Multipart form	Drilling: Number of holes	Drilling: Position	Drilling: Diameter	Drilling: Inches center to center	Drilling: Inches from edge	Padding: Position	Padding: Sets must register	Padding: Chipboard Required	Padding: Sheets per pad	Padding: Sets per pad	Padding: Sheets per set	Finishing: Perforation
93	1/4	White	20	CW Writing	Black	No							No	No				No
94	1/4	White	20	CW Writing	Black	No							No	No				No
95	1/4	White	20 lb	CW Writing	Black	No												
96	1/4	Buff	20 lb	CW Writing	Black	No												Yes
97																		
98	1	White	20 lb	CW Writing	Black	No												
99		White	16 lb	CW Writing	Black	No							No	No				No
100	1/2	White	20 lb	CW Writing	Black	No							No	No				Yes
101		White	16	CW Writing	Black	No							No	No				No
102	3/4	White	20	CW Writing	Black	No												

Printed Items Specification data table / Printed Form Products

	AG	AH	AI	AJ	AK	AL	AM
1	Finishing: Perforation: Position	Finishing: Score	Finishing: Score: Position	Serial Numbering: Start	Serial Numbering: End	Serial Numbering: Ink Color	Comment
2		No					Part 1 - NCR CB 15 lb White Part 2 - NCR CFB 17 lb Pink Part 3 - NCR CFB 17 lb Yellow Part 4 - NCR CFB 17 lb White Part 5 - NCR CF 17 lb White Hole drilling on Parts 1 - 3 and 5.
3		No					Part 1 - NCR CB 15 lb White Part 2 - NCR CFB 17 lb Pink Part 3 - NCR CFB 17 lb Yellow Part 4 - NCR CFB 17 lb White Part 5 - NCR CF 17 lb White Hole drilling on Parts 1 - 3 and 5.
4		No					Hole drilling is for Parts 1, 4, and 5 only.
5							
6	17" left	No					
7	17" from left						
8	17" from left flat size edge (pages 5 and 6)	No					Margins are as follows: Page 1 (L-1/2”X T-1/2”) Page 2 (L-1/2” X T-1/4”) Page 3 (L-1/8” X T-1/4”) Page 4 (L-3/16” X T-1/4”) Page 5
9							
10							
11							
12							
13							
14		No					

Printed Items Specification data table / Printed Form Products

	AG	AH	AI	AJ	AK	AL	AM
1	Finishing: Perforation: Position	Finishing: Score	Finishing: Score: Position	Serial Numbering: Start	Serial Numbering: End	Serial Numbering: Ink Color	Comment
15	On fold at 5 1/2"	No					
16	on fold at 5 1/2" from left	No					
17		No					
18						Red	
19	Multiple	Yes	Top and bottom covers to be scored on all folds				
20	Page 7 and 8 only - 1/4" from left edge						
21		No					
22							
23		No					
24							
25							
26							
27		No					
28		No					
29							
30		No					100/Shrink Film Suitable Carton
31		No					
32							
33							

Printed Items Specification data table / Printed Form Products

	AG	AH	AI	AJ	AK	AL	AM
1	Finishing: Perforation: Position	Finishing: Score	Finishing: Score: Position	Serial Numbering: Start	Serial Numbering: End	Serial Numbering: Ink Color	Comment
34							
35							
36		No					
37							
38							
39	7" from left						
40		No					
41	1/4" from left on pages 1 and 2 only.	No					
42	1/4" from left edge on pages 1 and 2 only	No					Page 1 top margin is 5/8". Page 3 top margin is 1/8" all other face page top margins are 1/4"
43	1/4" perf from left edge on pages 1 and 2 only	No					
44	1/4" from left edge pages 1 and 2 only	No					
45	1/4	No					
46	1/4	No					
47	1/4" from left on pages 1 and 2 only.	No					
48	1/4" from bind edge on pages 1 and 2 only	No					
49	1/4" from left on pages 1 and 2 only.	No					
50	1/4 from left on pages 1 and 2 only	No					
51	1/4" from left edge pages 1 and 2 only	No					
52	1/4" from left on pages 1 and 2 only	No					

Printed Items Specification data table / Printed Form Products

	AG	AH	AI	AJ	AK	AL	AM
1	Finishing: Perforation: Position	Finishing: Score	Finishing: Score: Position	Serial Numbering: Start	Serial Numbering: End	Serial Numbering: Ink Color	Comment
53		No					
54	1/4" from left edge on pages 1 and 2 only	No					
55		No					
56							
57		No					
58		No					
59		No					
60							
61		No					
62		No					
63							
64	1/4" from left edge on pages 1 and 2 only	No					
65							
66	1/4" perf from left edge on pages 9 and 10 only	No					
67		No					
68		No					
69							
70							
71		No					Perf 1/4" from left side Pgs 11 & 12
72							
73		No					Page 1 is NCR CB Page 2 is NCR CF both 15# paper
74							
75							

Printed Items Specification data table / Printed Form Products

	AG	AH	AI	AJ	AK	AL	AM
1	Finishing: Perforation: Position	Finishing: Score	Finishing: Score: Position	Serial Numbering: Start	Serial Numbering: End	Serial Numbering: Ink Color	Comment
76	17" from left on pages 5 and 6 only.	No					
77							
78		No					
79	8.5" left	No					
80							
81	Three (3) Perforations; first 3-1/4" from top, second: 5-1/8" from top, third: 8-3/8	No					
82							
83	8.5" from left.	No					
84	on fold at 8 1/2"	No					
85		No					
86							
87	1/4" from left edge on pages 23 and 24 only	No					
88	1/4" from left on pages 11 and 12	No					
89							
90							
91	1/4" from left edge on pages 11 and 12 only	No					
92	1/4" from left on pages 9-12.	No					

Printed Items Specification data table / Printed Form Products

	AG	AH	AI	AJ	AK	AL	AM
1	Finishing: Perforation: Position	Finishing: Score	Finishing: Score: Position	Serial Numbering: Start	Serial Numbering: End	Serial Numbering: Ink Color	Comment
93		No					
94		No					Two printed versions; (1) has holes and is not folded and (2) no holes and is a tri-fold product. Specs listed above are the basics and do not include holes/folding specs.
95							
96	17" from left						
97							
98							
99		No					
100	1/4" from left edge on pages 1 and 2 only.	No					
101		No					
102							

Printed Items Specification data table / Printed Publication Products

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Publication Number	Format	Publication Type	Number of Pages	Flat Size: Width	Flat Size: Height	Finished Size: Width	Finished Size: Height	Four Color Process (Full-Color)	Ink Colors: 1	Ink Colors: 2	Ink Colors: 3	Ink Colors: 4
2	05-10002	Format	Leaflet	2	24.5 x 8				No	295	2925		
3	05-10003	Format F	Fact Sheet	2					No	4725 U	295 U		
4	05-10005	Format F	Fact Sheet	2					No	4725 U	295 U		
5	05-10006	Format K	Leaflet	10	17.5 x 8				No	4725 U	295 U		
6	05-10007	Format F	Fact Sheet	2					No	327 U	295 U		
7	05-10008	Format F	Fact Sheet	2					No	2587 U	295 U		
8	05-10017	Format F	Fact Sheet	2					No	4725 U	295 U		
9	05-10018	Format I	Leaflet	2	10.5 x 8				No	377 U	295 U		
10	05-10021	Format F	Fact Sheet	2					No	4725 U	295 U		
11	05-10022	Format F	Fact Sheet	2					No	4725 U	295 U		
12	05-10023	Format J	Leaflet	8	14 x 7				No	4725 U	295 U		
13	05-10024	Format O	Booklet	32	5.25	8			No	4725	295		
14	05-10025	Format O	Booklet	36	5.25	8			No	4725 U	295 U		
15	05-10026	Format N	Booklet	20	3.5	8			No	377 U	295 U		
16	05-10029	Format O	Booklet	20	5.25	8			No	377 U	295 U		
17	05-10030	Format N	Booklet	24	3.5	8			No	377 U	295 U		
18	05-10031	Format F	Fact Sheet	1					No	4725 U	295 U		
19	05-10032	Format H	Leaflet	4	7 x 8				No	4725 U	295 U		
20	05-10034	Format J	Leaflet	8	14 x 7				No	186 U	295 U		
21	05-10035	Format O	Booklet	24	5.25	8			No	327 U	295 U		
22	05-10041	Format F	Fact Sheet	2					No	377 U	295 U		
23	05-10043	Format O	Booklet	24	5.25	8			No	144 U	295 U		
24	05-10045	Format F	Fact Sheet	2					No	327	295		
25	05-10046	Format F	Fact Sheet	2					No	377 U	295 U		
26	05-10052	Format O	Booklet	16	5.25	8			No	377 U	295 U		
27	05-10053	Format I	Leaflet	6	10.5 x 8				No	377 U	295 U		
28	05-10056	Format F	Fact Sheet	2					No	186 U	295 U		
29	05-10058	Format J	Leaflet	8	14 x 7				No	377 U	295 U		
30	05-10060	Format F	Fact Sheet	2					No	377 U	295 U		
31	05-10061	Format N	Booklet	20	3.5	8			No	377 U	295 U		
32	05-10062	Format F	Fact Sheet	2					No	377 U	295 U		
33	05-10063	Format F	Fact Sheet	2					No	327 U	295 U		
34	05-10064	Format J	Leaflet	8	14 x 7				No	2925 U	295 U		
35	05-10065	Format F	Fact Sheet	2					No	377 U	295 U		
36	05-10068	Format F	Fact Sheet	2					No	377 U	295 U		
37	05-10069	Format K	Leaflet	10	17.5 x 8				No	377 U	295 U		
38	05-10070	Format F	Fact Sheet	2					No	327 U	295 U		
39	05-10072	Format J	Leaflet	8	14 x 7				No	4725 U	295 U		
40	05-10073	Format J	Leaflet	8	14 x 7				No	4725 U	295 U		
41	05-10075	Format F	Fact Sheet	2					No	377 U	295 U		
42	05-10076	Format O	Booklet	20	5.25	8			No	4725 U	295 U		
43	05-10077	Format O	Booklet	32	5.25	8			No	4725 U	295 U		

Printed Items Specification data table / Printed Publication Products

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Publication Number	Format	Publication Type	Number of Pages	Flat Size: Width	Flat Size: Height	Finished Size: Width	Finished Size: Height	Four Color Process (Full-Color)	Ink Colors: 1	Ink Colors: 2	Ink Colors: 3	Ink Colors: 4
44	05-10081	Format F	Fact Sheet	2					No	4725 U	295 U		
45	05-10084	Format O	Booklet	16	5.25	8			No	2587 U	295 U		
46	05-10085	Format F	Fact Sheet	2					No	4725 U	295 U		
47	05-10087	Format H	Leaflet	4	7 x 8				No	377 U	295 U		
48	05-10090	Format K	Leaflet	10	17.5 x 8				No	377 U	295 U		
49	05-10093	Format F	Fact Sheet	2					No	2925 U	295 U		
50	05-10095	Format N	Booklet	24	3.5	8			No	377 U	295 U		
51	05-10096	Format F	Fact Sheet	2					No	2925 U	295 U		
52	05-10097	Format I	Leaflet	6	10.5 x 8				No	4725 U	295 U		
53	05-10100	Format K	Leaflet	10	17.5 x 8				No	4725 U	295 U		
54	05-10101	Format F	Fact Sheet	2					No	4725 U	295 U		
55	05-10105	Format F	Fact Sheet	2					No	4725 U	295 U		
56	05-10111	Format F	Fact Sheet	2					No	144 U	295 U		
57	05-10121	Format F	Fact Sheet	2					No	186	295		
58	05-10125	Format F	Fact Sheet	2					No	144 U	295 U		
59	05-10127	Format O	Booklet	24	5.25	8			No	4725 U			
60	05-10133	Format K	Leaflet	10	17.5 x 8				No	4725 U	295 U		
61	05-10137	Format N	Booklet	40	3.5	8			No	4725 U	295 U		
62	05-10138	Format N	Booklet	48	3.5	8			No	4725 U	295 U		
63	05-10147	Format F	Fact Sheet	2					No	327 U	295 U		
64	05-10148	Format F	Fact Sheet	2					No	327 U	295 U		
65	05-10153	Format O	Booklet	28	5.25	8			No	377 U	295 U		
66	05-10158	Format O	Booklet	20	5.25	8			No	4725 U	295 U		
67	05-10288	Format F	Fact Sheet	1					No	295 U	4725 U		
68	05-10501	Format F	Fact Sheet	2					No	1675 U	295 U		
69	05-10503	Format F	Fact Sheet	2					No	1675 U	295 U		
70	05-10504	Format I	Leaflet	6	10.5 x 8				No	4725 U	295 U		
71	05-10507	Format F	Fact Sheet	2					No	144 U	295 U		
72	05-10508	Format O	Booklet	20	5.25	8			No	144 U	295 U		
73	05-10510	Format H	Leaflet	4	7 x 8				No	186 U	295 U		
74	05-10511	Format F	Fact Sheet	2					No	186 U	295 U		
75	05-10512	Format F	Fact Sheet	2					No	2925 U	295 U		
76	05-10513	Format F	Fact Sheet	2					No	2925 U	295 U		
77	05-10514	Format F	Fact Sheet	2					No	2925 U	295 U		
78	05-10515	Format F	Fact Sheet	2					No	2925 U	295 U		
79	05-10516	Format I	Leaflet	6	10.5 x 8				No	186 U	295 U		
80	05-10517	Format	Leaflet	12	24.5 x 8				No	4725 U	295 U		
81	05-10521	Format F	Fact Sheet	2					No	144 U	295 U		
82	05-10522	Format I	Leaflet	6	10.5 x 8				No	327 U	295 U		
83	05-10523	Format F	Fact Sheet	2					No	144 U	295 U		
84	05-10525	Format I	Leaflet	6	10.5 x 8				No	144 U	295 U		
85	05-10529	Format F	Fact Sheet	2					No	144 U	295 U		

Printed Items Specification data table / Printed Publication Products

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Publication Number	Format	Publication Type	Number of Pages	Flat Size: Width	Flat Size: Height	Finished Size: Width	Finished Size: Height	Four Color Process (Full-Color)	Ink Colors: 1	Ink Colors: 2	Ink Colors: 3	Ink Colors: 4
86	05-10530	Format J	Leaflet	8	14 x 7				No	144 U	295 U		
87	05-10531	Format F	Fact Sheet	2					No	144 U	295 U		
88	05-10535	Format F	Fact Sheet	1					No	PMS 301	PMS 186		
89	05-10540	Format F	Fact Sheet	2					No	186 U	295 U		
90	05-10550	Format I	Leaflet	6	10.5 x 8				No	377 U	295 U		
91	05-10552	Format F	Fact Sheet	2					No	186 U	295 U		
92	05-10561	Format F	Fact Sheet	2					No	186 U	295 U		
93	05-10900	Format J	Leaflet	8	14 x 7				No	1675 U	295 U		
94	05-10902	Format	Leaflet	14	24.5 x 8				No	327 U	295 U		
95	05-10903	Format O	Booklet	28	5.25	8			No	377 U	295 U		
96	05-10906	Format L	Leaflet	12	21 x 8				No	295 U	4725 U		
97	05-10907	Format F	Fact Sheet	2					No	327 U	295 U		
98	05-10910	Format F	Fact Sheet	2					No	295 U	144 U		
99	05-10913	Format K	Leaflet	10	17.5 x 8				No	295 U	4725 U		
100	05-10915	Format N	Booklet	28	3.5	8			No	295 U	1675 U		
101	05-10917	Format F	Fact Sheet	2					No	4725 U	295 U		
102	05-10918	Format I	Leaflet	6	10.5 x 8				No	377 U	295 U		
103	05-10921	Format F	Fact Sheet	2					No	4725 U	295 U		
104	05-10922	Format F	Fact Sheet	2					No	295 U	4725 U		
105	05-10923	Format K	Leaflet	10	17.5 x 8				No	295 U	4725 U		
106	05-10925	Format I	Leaflet	6	10.5 x 8				No	144 U	295 U		
107	05-10927	Format O	Booklet	32	5.25	8			No	295 U	4725 U		
108	05-10929	Format O	Booklet	24	5.25	8			No	377 U	295 U		
109	05-10931	Format F	Fact Sheet	2					No	295 U	4725 U		
110	05-10935	Format O	Booklet	28	5.25	8			No	327 U	295 U		
111	05-10941	Format F	Fact Sheet	2					No	377 U	295 U		
112	05-10943	Format O	Booklet	24	5.25	8			No	144 U	295 U		
113	05-10953	Format I	Leaflet	6	10.5 x 8				No	377 U	295 U		
114	05-10958	Format J	Leaflet	8	14 x 7				No	377 U	295 U		
115	05-10961	Format N	Booklet	20	3.5	8			No	377 U	295 U		
116	05-10964	Format K	Leaflet	10	17.5 x 8				No	295 U	2925 U		
117	05-10968	Format F	Fact Sheet	2					No	295 U	377 U		
118	05-10975	Format F	Fact Sheet	2					No	295 U	377 U		
119	05-10976	Format O	Booklet	24	5.25	8			No	295 U	4725 U		
120	05-10977	Format O	Booklet	36	5.25				No	295 U	4725 U		
121	05-10978	Format L	Leaflet	12	21 x 8				No	295 U	4725 U		
122	05-10984	Format O	Booklet	20	5.25	8			No	2587 U	295 U		
123	05-10985	Format F	Fact Sheet	2					No	295 U	4725 U		
124	05-10987	Format H	Leaflet	4	7 x 8				No	377 U	295 U		
125	05-10989	Format F	Fact Sheet	2					No	144 U	295 U		
126	05-10990	Format L	Leaflet	12	21 x 8				No	377 U	294 U		
127	05-10991	Format F	Fact Sheet	2					No	295 U	144 U		

Printed Items Specification data table / Printed Publication Products

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Publication Number	Format	Publication Type	Number of Pages	Flat Size: Width	Flat Size: Height	Finished Size: Width	Finished Size: Height	Four Color Process (Full-Color)	Ink Colors: 1	Ink Colors: 2	Ink Colors: 3	Ink Colors: 4
128	05-10992	Format F	Fact Sheet	2					No	295 U	144 U		
129	05-10993	Format F	Fact Sheet	2					No	295 U	2925 U		
130	05-10996	Format F	Fact Sheet	2					No	295 U	2925 U		
131	05-10997	Format K	Leaflet	10	17.5 x 8				No	295 U	377 U		
132	05-10998	Format I	Leaflet	6	10.5 x 8				No	327 U	295 U		
133	05-10999	Format J	Leaflet	8	14 x 7				No	295 U	144 U		
134	05-11000	Format O	Booklet	16	5.25	8			No	1675 U	295 U		
135	05-11005	Format N	Booklet	20	3.5	8			No	295 U	1675 U		
136	05-11008	Format K	Leaflet	10	17.5 x 8				No	295 U	1675 U		
137	05-11011	Format O	Booklet	32	5.25	8			No	295 U	1675 U		
138	05-11015	Format O	Booklet	36	5.25	8			No	1675 U	295 U		
139	05-11017	Format K	Leaflet	10	17.5 x 8				No	377 U	295 U		
140	05-11024	Format O	Booklet	36	5.25	8			No	1675 U	295 U		
141	05-11051	Format F	Fact Sheet	2					No	1675 U	295 U		
142	05-11052	Format F	Fact Sheet	2					No	1675 U	295 U		
143	05-11069	Format I	Leaflet	6	10.5 x 8				No	295 U	1675 U		
144	05-11070	Format I	Leaflet	6	10.5 x 8				No	1675 U	295 U		
145	05-11090	Format O	Booklet	16	5.25	8			No	295 U	1675 U		
146	05-11098	Format K	Leaflet	10	17.5 x 8				No	295 U	1675 U		
147	70-10281		Leaflet	2					No	295	1675		

EXHIBIT O

Initial Stock Retrieval Report / Sample Retrieving Report

	A	B	C	D	E	F
1	Product_ID	Edition_Date	Product_Type	Quantity	Current_Unit_of_Issue	Repackage_Unit_of_Issue
2	552500		O	1000	Each	
3	05-10550	01/2020	P	5000	Package of 100	Package of 25
4	SS-5	02/2020	F	150000	Package of 100	Package of 25
5	ENV-00025		E	200000	Case of 500	

Initial Stock Retrieval Report / Data Spec

	A	B	C	D	E
1	Product_ID	Edition_Date	Product_Type	Quantity	Current_Unit_of_Issue
2	Product ID of the item being retrieved	Edition date of the product being retrieved	P = Publication F = Form E = Envelope O = Other	Quantity being retrieved	This is the unit of issue that the item is currently packaged in when retrieved.
3					

Initial Stock Retrieval Report / Data Spec

	F
1	Repackage_Unit_of_Issue
2	This is the unit of issue the contractor will repackage the product after retrieval.
3	If this is blank then the product will not need to be repackaged

EXHIBIT P

Order Date: <Order Date>

Order #: <MyStock Order Number>

Ship Method: <Shipping Method>

Packing Slip

SHIP TO:

MS
DDS
P O BOX 1271
JACKSON, MS 39215-

NOTES:

ITEM ID	QUANTITY	DESCRIPTION
05-11008	500	Your Right to Questions The Decision Made On Your SSI Claim

EXHIBIT Q

SOCIAL SECURITY ADMINISTRATION

CERTIFICATE OF SELECTION

OF

"YELLOW LABEL" RANDOM COPIES

I hereby certify that the random copies produced under Jacket_____(Program_____P.O._____)

by_____ have been selected in accordance with the selection plan specified.
(Name of Company)

I understand that these random copies will be inspected against the attributes specified in the contract.

The penalty for making false statements to the U.S. Government is prescribed in 18 U.S.C. 1001.

_____
(Signature of Certifying Official) *(Date)*

_____
(Printed Name and Title of Certifying Official)

Instructions:

- The contractor must select random copies in accordance with the specified selection plan.
- A dated copy of this form, signed by an authorized company official **and a copy of the specifications** must be included with the shipment.
- Random copies, certificate **and specifications** must be forwarded in accordance with the attached mailing label.

CPP/PMB/032210/Rev.

FROM:	FOR USPS DELIVERY APPLY POSTAGE

AGENCY	INTERNAL CONTROL NUMBER (ICN)
REQUISITION NO.	IN-HOUSE REQUISITION NO.
GPO JACKET NO.	TITLE
GPO ORDER NO.	PRODUCT DESCRIPTION
PROGRAM and PRINT ORDER NO.	
FORM or PUBLICATION NO. and DATE	TO:
QUANTITY PER CONTAINER	
PACKAGES PER CONTAINER OF	

YELLOW LABEL SAMPLE 8-Social Security Administration

OF/PMR/3ZZ1D-1

< Trim Off Warning Paragraph Before Reproducing This Label >

WARNING TO CONTRACTORS! ***PLEASE DO NOT USE THIS YELLOW LABEL WHEN MAILING OR SHIPPING BLUE LABEL SAMPLES TO THE SOCIAL SECURITY ADMINISTRATION. USE THE ORIGINAL BLUE LABELS YOU NORMALLY ATTACH TO BLUE LABEL SAMPLES SHIPPING CONTAINERS. THANK YOU!***