PRG:	**837-S**									
TITLE:	**Customer Satisfaction Survey Packets**									
AGENCY:	**Department of the Treasury / IRS**									
TERM:	**Beginning Date of Award and ending May 31, 2025**								**CURRENT CONTRACTOR**	
									DATA RECOGNITION CORP.	
			ADVANTAGE MAILING LLC.		**CUEST CORP.**		**NPC, INC.**		**Maple Grove, MN**	
		BASIS OF	Anaheim, CA				Claysburg, PA			
ITEM NO.	DESCRIPTION	**AWARD**	UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**	UNIT RATE	**COST**
I.	**ELECTRONIC PREPRESS:**									
(a)	PDF Proof.....per file....	80	N/C	**-**	40.00	**3,200.00**	N/C	**-**	N/C	**-**
(b)	Digital color content or Digital one-off proofs									
	.....per trim/page-size unit...	80	15.000	**1,200.00**	65.00	**5,200.00**	N/C	**-**	N/C	**-**
(c)	Prior-to-production samples...per trim/page-size unit...	80	15.000	**1,200.00**	45.00	**3,600.00**	N/C	**-**	N/C	**-**
II.	**PRINTING/VARIABLE IMAGING, BINDING,**									
	CONSTRUCTION, PACKAGE ASSEMBLY, AND									
	DISTRIBUTION:									
(a)	**Two-Page Survey (8-1/2 x 11") Catergory 1:**									
	Printing face and back in black ink and imaging face only									
	in black ink, including binding.....per survey.....	431,758	0.330	**142,480.14**	4.85	**2,094,026.30**	0.13	**56,128.54**	0.108	**46,716.22**
(b)	**Two-Page Survey (8-1/2 x 11") Catergory 2:**									
	Printing face and back in black ink and one									
	Pantone ink color and imaging on first page in black ink,									
	including binding.....per survey.....	24,926	0.330	**8,225.58**	7.06	**175,977.56**	0.32	**7,976.32**	0.152	**3,778.78**
(c)	**Four-Page Survey (17 x 11"):**									
	Printing face and back in black ink and one Pantone									
	ink color and imaging on first page in black ink,									
	including binding.....per survey.....	73,751	0.660	**48,675.66**	10.50	**774,385.50**	0.34	**25,075.34**	0.200	**14,728.07**
(d)	**Pre-Note:**									
	Printing face only in black ink and imaging face only in									
	black ink, including binding.....per pre-note.....	252,834	0.220	**55,623.48**	5.30	**1,340,020.20**	0.22	**55,623.48**	0.071	**17,925.93**
(e)	**Letters:**									
	Printing face only in black ink and imaging face only									
	in black ink, including binding.....per letter.....	539,794	0.330	**178,132.02**	4.81	**2,596,409.14**	0.25	**134,948.50**	0.075	**40,322.61**
(f)	**Standard Postcard:**									
	Printing face and back in black ink and imaging face only									
	in black ink, including binding.....per postcard.....	272,489	0.110	**29,973.79**	1.33	**362,410.37**	0.04	**10,899.56**	0.042	**11,526.28**
(g)	**Folded Postcard:**									
	Printing face and back in black ink and imaging									
	in black ink, including binding.....per postcard.....	98,237	0.220	**21,612.14**	3.27	**321,234.99**	0.31	**30,453.47**	0.139	**13,654.94**
(h)	**Business Reply Envelope (No. 9):**									
	Printing in a single ink color, including construction									
	.....per envelope.....	526,472	0.050	**26,323.60**	1.52	**800,237.44**	0.04	**21,058.88**	0.016	**8,423.55**
(i)	**Mailing Window Envelope (No. 10):**									
	Printing in a single ink color, including construction									
	.....per envelope.....	799,298	0.050	**39,964.90**	1.80	**1,438,736.40**	0.04	**31,971.92**	0.028	**22,380.34**
III.	**ADDITIONAL OPERATIONS:**									
	Programming.....per hour.....	23	N/C	**-**	56.00	**1,288.00**	100.00	**2,300.00**	150.00	**3,450.00**
	CONTRACTOR TOTALS			**$ 551,011.31**		----------		**$ 376,436.01**		**$ 182,906.74**
	DISCOUNT		0.25%	**$ 1,377.53**			0.25%	**$ 941.09**		**$ -**
	DISCOUNTED TOTALS			**$ 549,633.78**		----------		**$ 375,494.92**		**$ 182,906.74**
							AWARDED			

GPO Antonio Mozie
Contracting Officer

since 1861

June 6, 2024

This is Amendment No. 1. The specifications in our invitation for bids on Program 837-S, scheduled for opening at 11:00 AM EST on June 20, 2024, are amended as follows:

1. On pages 33 and 34 of 35 under "PRINTING/VARIABLE IMAGING, BINDING, CONSTRUCTION, PACKAGE ASSEMBLY, AND DISTRIBUTION:" Delete the following:
   - Fractional parts of 100 will be prorated at the per-100 rate.
   - Running Per 100 Copies

All other specifications remain the same.

If amendment is not acknowledged on bid, direct acknowledgment to:

U.S. Government Publishing Office
Bid Section, Room C848, Stop CSPS
732 North Capitol Street NW
Washington, DC 20401-0001

Amended bid or acknowledgement must be submitted using the method(s) specified in the solicitation for bid submission. Telephone or e-mail submission is not acceptable.

BIDDER MUST ACKNOWLEDGE RECEIPT OF THIS AMENDMENT PRIOR TO BID OPENING. Failure to acknowledge receipt of amendment, by amendment number, prior to bid-opening time, may be reason for bid being declared nonresponsive.

Sincerely,

Antonio Mozie

Digitally signed by Antonio Mozie
Date: 2024.06.06 12:54:07 -04'00'

Antonio Mozie
Contracting Officer

GPO **Antonio Mozie**
Contracting Officer

since 1861

June 6, 2024

This is Amendment No. 1. The specifications in our invitation for bids on Program 837-S, scheduled for opening at 11:00 AM EST on June 20, 2024, are amended as follows:

1. On pages 33 and 34 of 35 under "PRINTING/VARIABLE IMAGING, BINDING, CONSTRUCTION, PACKAGE ASSEMBLY, AND DISTRIBUTION:" Delete the following:
   - Fractional parts of 100 will be prorated at the per-100 rate.
   - Running Per 100 Copies

All other specifications remain the same.

If amendment is not acknowledged on bid, direct acknowledgment to:

U.S. Government Publishing Office
Bid Section, Room C848, Stop CSPS
732 North Capitol Street NW
Washington, DC 20401-0001

Amended bid or acknowledgement must be submitted using the method(s) specified in the solicitation for bid submission. Telephone or e-mail submission is not acceptable.

BIDDER MUST ACKNOWLEDGE RECEIPT OF THIS AMENDMENT PRIOR TO BID OPENING. Failure to acknowledge receipt of amendment, by amendment number, prior to bid-opening time, may be reason for bid being declared nonresponsive.

Sincerely,

Antonio Mozie
Contracting Officer

U.S. GOVERNMENT PUBLISHING OFFICE
Washington, DC

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

Customer Satisfaction Survey Packets

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

Department of the Treasury/Internal Revenue Service (IRS)

Single Award

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

The period from Date of Award to September 30, 2024, will be used by the contractor to comply with the IRS security requirements and personnel screening investigations. Actual, live production begins on or around October 1, 2024. 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 June 20, 2024, 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 of the products ordered under this contract must be located within the continental United States.

BIDDERS, PLEASE NOTE: ***This program was formerly Program 290-S.*** These specifications have been extensively revised; therefore, all bidders are cautioned to familiarize themselves with all provisions of these specifications before bidding.

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 Cecilia Dominguez Castro at (202) 512-0418 or at cdominguezcastro@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 Pub. 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.p

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

SUBCONTRACTING: The provisions of GPO Publication 310.2 are modified to permit subcontracting for the manufacturing of the envelopes only.

GPO IMPRINT REQUIREMENT: The GPO imprint requirement, GPO Contract Terms, Supplemental Specification, No. 9, is waived.

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

Product Quality Levels:

(a) Printing (page related) Attributes - Level III. (See "PRINTING AND VARIABLE IMAGING.")
(b) Finishing (item related) Attributes - Level III.

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

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

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

Attribute	Specified Standard
P-7. Type Quality and Uniformity	O.K. Prior-to-Production Samples/O.K. Proofs/ Average Type Dimension/Electronic Media
P-9. Process Color Match	Pantone Matching System

Prior to award, contractor may be required to provide information related to specific equipment that will be used for production.

OPTION TO EXTEND THE TERM OF THE CONTRACT: The Government has the option to extend the term of this contract for a period of 12 months by written notice to the contractor not later than 30 days before the contract expires. If the Government exercises this option, the extended contract shall be considered to include this clause, except, the total duration of the contract may not exceed five (5) years as a result of, and including, any extension added under this clause. Further extension may be negotiated under the "EXTENSION OF CONTRACT TERM" clause. See also "ECONOMIC PRICE ADJUSTMENT" for authorized pricing adjustments(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 a 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 May 31, 2025, 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 February 29, 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.

SECURITY REQUIREMENTS: The contractor shall comply with all security requirements set forth in these specifications as well as all IRS-specific security requirements as specified in Attachment 1.

NOTE: All furnished data is designated as "Sensitive But Unclassified" (SBU) and contains "Personally Identifiable Information" (PII).

SECURITY WARNING: Proper control and handling must be maintained at all times to prevent any information or materials required to produce the product ordered under these specifications from falling into unauthorized hands. All Sensitive But Unclassified data must be adequately protected and secured and meet the required physical security minimum protection standards as defined in the latest revisions of Publications 4812 and 4812-A. Unless otherwise indicated herein, all extra copies, materials, waste, etc., must be destroyed in accordance with IRS Publications 4812 and 4812-A. Links to these publications are found in Exhibit J).

The contractor agrees that it shall establish and maintain full Secure Data Transfer (SDT) compliance throughout the term of this contract. Contractor receiving SBU information from the IRS shall meet the requirements set forth below, in accordance with the IRS Publications 4812, 4812-A and Federal Information Security Management Act (FISMA) Compliant Data Protection and Internal Revenue Code 6103(n):

(a) All federal, state, and local agencies or entities shall comply with IRS Publications, 4812, and 4812-A, if transmitted data contains Federal Taxpayer Information (FTI). All data that originates from the IRS shall be protected to ensure compliance with FISMA, including the technical security, physical security, personnel security, and record retention requirements. All IRS systems that handle or process Federal Tax Information (FTI) or other Sensitive but Unclassified (SBU) information, including Personally Identifiable Information (PII), source code, etc. are categorized at the moderate risk level, as required by Publication FIPS 199, Standards for Security Categorization of Federal Information and Information Systems. This contract handles FTI at the moderate risk level. The Government has the option to increase the risk level.

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

- Personal identification numbers, such as passport number, driver's license number, taxpayer identification number, or financial account or credit card number.
- Address information, such as street address or personal email address.
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), fingerprints, handwriting, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry).

Contractor shall comply with moderate risk controls of National Institute of Standards and Technology (NIST) SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 5. NIST is a Federal technology agency that develops and promotes measurement, standards, and technology. NIST also provides additional guidance, publications, and compliance tools to Government agencies at http://csrc.nist.gov/groups/SMA/fisma/index.html.

1. Authorized Data Recipients. Only authorized individuals may receive SBU information from the IRS. Individual identification and authentication will be accomplished through use of a third-party digital certificate issued by name to authorized individuals.

2. Data Tracking and Accounting. Contractor receiving SBU information are responsible for ensuring the security of SBU information within the firm and shall establish procedures to track and account for data from receipt to disposition. If the contracted entity is a federal, state, or local agency and transmitted data contains FTI, these procedures shall meet the requirements of Publications 4812, and 4812-A. Contractor shall ensure that the individual responsible for accounting for receipt of SBU information is provided with the "control file" that accompanies the extract file on SDT. The contractor is required to provide IRS with a separate acknowledgment of receipt of SBU information.

3. Data Transfer Log File. Contractor receiving SBU information must maintain a log file that records complete and incomplete data transfers. For complete transmissions, the log file must identify the sender of the information, the file name, the date/time of receipt, and the record count. For incomplete transfers, the log file must identify as much of the above information as possible.

4. Confirmation of Successful Data Transfers and Record Count. When a contractor receives a file from the IRS via SDT, the contractor shall check the file to see that it is intact and usable; the contractor shall also validate the record count provided on the "control file." In the event of incomplete or unsuccessful transfers, including a file where record counts cannot be validated, the contractor shall notify the IRS immediately and request that the file be retransferred. Requests for retransfer shall include the following information: Name, phone number, and email address of the person making the request; name, phone number and email address of an alternate contractor contact; file name, job run file ID number, and complete contractor name.

5. Sensitive but Unclassified (SBU) Information Breach/Misrouted File. An SBU information breach includes any incident where SBU data is lost, misused, or compromised. This includes but is not limited to situations involving a misrouted file (a file meant for one entity or contractor is received by another entity or contractor) containing SBU data.

   Security and Privacy incidents related to IRS processing, IRS SBU data, or contractor information systems shall be reported ***immediately*** upon discovery to the GPO at cdominguezcastro@gpo.gov; the IRS contracting representatives Erika Bryant, (470) 769-2030, Erika.J.Bryant@irs.gov, Sylvia Greene, (470) 639-2480, Sylvia.J.Greene@irs.gov, and Brandis Dew (313) 234-2498, Brandis.S.Dew@irs.gov; and the Computer Security Incident Response Center (CSIRC) Incident Response Operations Team at (240) 613-3606. The IRS Contracting Officer Representative (COR) shall complete the Computer Security Incident Reporting (CSIR) Form available at https://www.csirc.web.irs.gov/reporting/. The Government will take appropriate action and advise the contractor of further action, if any, required by the contractor and/or consequences resulting from the SBU Breach.

   In addition, if the SBU information is or involves returns, return information, or threatens the safety or security of personnel or information systems, the contractor shall report the incident/situation to the Treasury Inspector General for Tax Administration (TIGTA) hotline at (800) 366-4484.

   This is also part of IRS Security Clause IR1052.224-9000. The Government will take appropriate action and advise the contractor of further action, if any, required by the contractor and/or consequences resulting from the SBU Breach.

6. Access Controls and Audit Logs. The contractor shall ensure that any information system (server, workstation, laptop, etc.) storing SBU information maintains access controls to the information and audit logs that document any access to the information in accordance with NIST SP 800-53. Audit logs must be saved for seven (7) years. For all federal, state, and local agencies or entities, if data transmitted through the SDT and stored on the agency's system contains FTI, access to the information shall be recorded and reviewed, as identified for access controls and auditing within Publications 4812 and 4812-A.

7. Validation of Authorized Users. All logical access to IRS information shall be controlled by U.S. Government-approved authentication methods to validate the authorized users.

8. Web Accessible File Sharing Support. There shall be no dial-up or broadband support for web-accessible file sharing. Remote administration of the web-accessible file-sharing systems is permitted only via FIPS 140-2 compliant products.

9. Safeguard Disclosure of Federal Taxpayer Information (FTI) Data Transmitted Through The Secure Data Transfer (SDT). If SDT is used by the contractor to receive FTI data from the IRS, a revised Safeguard Procedures Report (SPR) is not required to participate in SDT. The contractor's next annual Safeguard Activity Report (SAR) submission shall document all protection mechanisms used to secure and store all data received in performing this contract. This shall include identifying the protection procedures, as well as the destruction procedures for data files received via SDT.

10. All SBU must be protected at rest, in transit, and in exchanges (i.e., internal and external communications). The contractor shall employ encryption methods and tools to ensure the confidentiality, integrity, and availability of SBU information.

11. Contractor shall ensure that all laptops being used for this contract use full disk encryption.

(b) All IT assets must be configured to ensure compliance with the NIST Security Content Automation Protocol (SCAP) located on the NIST web site.

In addition, the contractor must comply with all IRS Security Clauses as specified in Attachment 1.

NOTE: Contractor must comply with IR1052.204-9002 IRS SPECIALIZED INFORMATION TECHNOLOGY (IT) SECURITY TRAINING (ROLE-BASED) REQUIREMENTS (JUN 2022), (see Attachment 1). The contractor is responsible for any costs incurred to meet the specialized role-based training requirements.

DATA RIGHTS: All data and materials furnished and produced in the performance of this contract shall be the sole property of the Government. The contractor agrees not to assert rights or to establish any claim to such data in whole or in part in any manner or form, or to authorize others to do so, without prior written consent of the Contracting Officer.

Information contained in all source documents and other media provided by the Government is the sole property of the Government.

WARNING: The contractor is prohibited from producing or distributing the products produced under this contract outside of the official orders (i.e., cannot produce for their own use, sale, or other uses, including marketing, promotion, or other uses).

The contractor shall not retain or distribute, in any form, any part of the materials furnished by the Government which are not consumed in the preparation of the work, or which are generated as a result of this contract. Proper precautions shall be taken to ensure that all Government-supplied materials are protected from damage. The Government-furnished materials shall be returned in the same condition as originally furnished (when applicable).

Proper control and handling must be maintained at all times to prevent any information, data, or materials required to produce the products ordered under these specifications from falling into unauthorized hands.

All erroneous copies produced by the contractor are to be destroyed by means of abrasive destruction, burning, shredding, or other methods that guarantee complete protection against access and in accordance with the level of security designated by the agency. (See "DISPOSAL OF WASTE MATERIALS.")

DISPOSAL OF WASTE MATERIALS: *Subcontracting for the disposal of waste materials will not be allowed*. The contractor is required to demonstrate how all waste materials used in the production of sensitive records containing SBU and PII data will be definitively destroyed (i.e., 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 exempted from disclosure by statute, including the Privacy Act or regulation. Contractor is required to show proof of disposal.

All disposal/destruction must be performed onsite at the contractor's secure production facility, close to the point of production. Any waste material containing PII that is not destroyed immediately must be stored in a secured area while awaiting destruction. A cover must be placed over any bins with waste material containing PII when being moved from one location to another within the contractor's facility. Sending intact waste containing PII to a municipal incinerator, a recycler, or any other off-site processor is not acceptable and will be considered a data breach.

Contractor must provide a destruction certificate to the IRS (when applicable).

PREAWARD SURVEY: In order to determine the responsibility of the prime contractor, the Government reserves the right to conduct an on-site preaward survey at the contractor'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)

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.

PREAWARD PLANS: The contractor shall present, in writing, to the Contracting Officer within three (3) workdays of being notified to do so by the Contracting Officer or his/her representative, detailed plans the following activities. The workday after notification to submit will be the first day of the schedule.

THESE PROPOSED PLANS ARE SUBJECT TO REVIEW AND APPROVAL BY THE GOVERNMENT, AND AWARD WILL NOT BE MADE PRIOR TO APPROVAL OF THE SAME. THE GOVERNMENT RESERVES THE RIGHT TO WAIVE ANY OR ALL OF THESE PLANS.

Option Years: For each option year that may be exercised, the contractor will be required to re-submit, in writing, the above plans detailing any changes and/or revisions that may have occurred. The contractor should be prepared to submit these plans to GPO within five (5) workdays of notification of the option year being exercised.

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

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

The plans must provide for periodic samplings to be taken during the production run and shall contain control systems that will detect defective, missing, mutilated, or mismatched items. The plans shall detail the actions to be taken by the contractor when defective, missing, mutilated, or mismatched items are discovered. These actions must be consistent with the requirements found in GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987 (Rev. 01-18)). The plan shall monitor all aspects of the job including material handling and mail flow, to assure that the production and delivery of the Survey Packets meet specifications and Government requirements. This includes maintaining 100% accountability in the accuracy of imaging and mailing of all pieces throughout each run. The contractor must ensure that there are no missing or duplicate pieces.

A recovery system will be required to ensure that all defective, missing, mutilated, or mismatched pieces detected are identified, reprinted, and replaced.

The quality control plan must also include examples and a detailed description of all reports or logs the contractor will keep, to document the quality control inspections performed on each run. Contractor must submit a quality control checklist for approval prior to award.

Furthermore, the plan must include the names of all quality assurance officials and describe their duties in relation to the quality control plan.

The Government may periodically verify that the contractor is complying with the approved quality control plan through on-site examinations and/or requesting copies of the contractor's quality assurance records and quality assurance random copies.

Mail Plan: This plan shall include sufficient detail as to how the contractor will comply with all applicable U.S. Postal Service (USPS) mailing requirements as listed in the USPS Domestic and International Mail Manuals in effect at the time of mailing and other USPS instructional material such as the Postal Bulletin. (See "DISTRIBUTION.")

Many of the mailing cycles occur simultaneously and overlap in production. When a revision (creating a new version) of a survey needs to take place, the contractor must have the following quality checks in place to ensure errors are avoided:

1. Validate with the IRS that the correct revision is in use and is correct and maintain a spreadsheet that shows revision histories.

2. Implement an enhanced quality check sheet that is used on each mailing. The check sheet will require the positive match of the form number against the print order and the actual print output as well as random checks on aesthetic items such as address placement.

3. Prior to mailing any revised pre-notification letters (herein after referred to as "pre-notes"), letters, surveys, and postcards, proofs and prior-to-production samples will be required for IRS approval, as required in SECTION 2. Receipt of the proof/prior-to-production sample approval will be required before the mailing can occur.

4. IRS will submit Form 14573 - Survey Checklist of Scanned Mail Components for the contractor to complete prior to mailing revised survey components.

NOTE: Revisions will be made at the beginning of a quarter.

Material Handling and Inventory Control: This plan shall explain in detail how the following materials will be handled: incoming data files; work-in-progress materials; quality control inspection materials; USPS inspection materials; and all outgoing materials cleared for USPS pick-up/delivery.

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

Production Plan: This plan shall include items such as a detailed listing of all production equipment and equipment capacities to be utilized in this contract. If new equipment is to be utilized, documentation of the source, delivery schedule, and installation dates are required.

Security Control Plan: This plan shall provide in detail, at a minimum:

- How all accountable materials will be handled throughout all phases of production.
- How all furnished data will be stored and protected.
- How the disposal of waste materials will be handled. (See "DISPOSAL OF WASTE MATERIALS.")
- List of contractor's employees involved and their specific function.
- How all applicable Government-mandated security/privacy/rules and regulations, as cited in this contract, shall be adhered to by the contractor.

- Production Area – The contractor must provide a secure area(s) dedicated to the processing and storage of data for the Survey Packets, separated from other work, as detailed in Publication 4812. Access to the area(s) shall be limited to security-trained and cleared employees involved in the production of the Survey Packets. Please refer to Publication 4812 occasionally to verify if the controls have changed.

The following items must be stored in locked containers:

- IRS Letterhead
- Survey components with variable data, such as pre-printed and packaged survey packets awaiting mailing.

(For further information, see Attachment 1 and Publication 4812 (see Exhibit J).

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

These documents will be reviewed and analyzed by both Physical Security and Cybersecurity and any other security components, if implicated, for completeness, accuracy, and compliance with security standards. Any questions identified during the analysis will be coordinated with the GPO for clarification and verification.

After coordination with security personnel, a recommendation on whether the contractor is able to meet the security standards will be made to GPO.

Physical Security and Cyber Security Self-Assessments: When the contractor is notified to present their production plans, they will be provided the Physical Security Self-Assessment and Cyber Security Self-Assessment via Microsoft Excel file format. Contractor must submit the completed self-assessments in conjunction with the production plans. (See Exhibit L and Exhibit M.)

PREAWARD TEST: The contractor being considered for award may be required to demonstrate their ability to produce the items required in these specifications at the requisite quality level by completing a preaward test. The Government reserves the right to waive the preaward test if there is other evidence that, in the opinion of the Contracting Officer, indicates that the contractor being considered for award has the capability to successfully produce the items required.

For the preaward test, electronic files representative of the files to be furnished under these specifications (consisting of all required components for each wave of a "test survey") will be furnished by the Government via email.

The preaward test samples must be of the type required by these specifications. Each sample shall be printed and constructed as specified and must be of the size, kind, and quality that the contractor will furnish.

The sample surveys, letters, postcards, and envelopes must be printed on the paper required under these specifications. NOTE: The pre-notes will be printed on the same paper as the letter for the preaward test only.

The contractor will be required to submit separate, complete packages of preaward test samples to 13 different addresses within the continental United States. Addresses will be provided at the time of testing.

The prospective contractor shall provide the following to <u>each</u> address:

- One (1) complete, assembled packet containing one sample of each required component for each wave of the furnished survey.

In addition, four (4) of these addresses shall receive:

- 10 additional samples of the survey component only to be tested on scanners.

NOTE: The sample surveys must be compatible for scanning on an Insight 70, Scantron Insight 700c, Fujitsu FI-5950, Fujitsu FI-7160 and Fujitsu fi-6800.

Preaward test samples must be submitted within seven (7) workdays of receipt of the Government furnished preaward test materials.

If preaward test samples are disapproved by the Government, the contractor may be permitted, at the option of the Government, additional time to correct defects and/or submit revised test samples, if so notified by the Contracting Officer. A maximum of TWO (2) attempts will be allowed.

In the event the revised preaward test samples are disapproved by the Government, the contractor shall be deemed to have failed to comply with the applicable requirements of these specifications and may be reason for a determination of non-responsibility.

Failure to deliver completed preaward test samples within the specified timeframe may disqualify the contractor from further consideration for award.

All operations necessary in the performance of this test shall be performed at the facilities and on the equipment in which the contract production will be performed.

No charges will be allowed for costs incurred in the performance of this preaward test.

PREAWARD AND 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 prospective contractor's/contractor's representatives at the contractor's plant or the U.S. Government Publishing Office, Washington, DC, immediately after award. At the Government's option, the preaward call and postaward conference calls may be held via teleconference.

The contractor will be contacted to set up several teleconference calls:

Preaward Call (estimated 1-1/2 hours) – IRS Cybersecurity and Physical Security will provide the prospective contractor with necessary forms and expectations leading up to the 1-hour Postaward Call 3 (see below).

Postaward Call 1 (estimated 1 hour) – Provided production plans and quality system plans will be discussed between IRS Publishing and the contractor. Attending this meeting will be representatives from the Internal Revenue Service and the Government Publishing Office.

Postaward Call 2 (estimated 1 hour) – IRS Personnel Security will discuss the information that is needed from the contractor for each employee working on this contract.

Postaward Call 3 (estimated 1 hour prior to the 3-day assessment) – Actual assessment of contractor by Cyber Security, Physical Security, and Personnel Security. Contractor will be given feedback on what was provided to the IRS. Discussion and review of all aspects of the contractor's internal and external operations required to complete this contract.

NOTE: To establish coordination of all required operations, representatives from each involved production area from the contractor should attend.

Option years: For each option year that may be exercised, the Government's representatives may request a meeting with the contractor's representatives to be held at the contractor's facility or via conference call to discuss the requirements of that contract year's jobs.

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

ORDERING: Items to be furnished under the contract shall be ordered by the issuance of print orders by the Government. Orders may be issued under the contract from Date of Award through May 31, 2025 plus for such additional period(s) as the contract is extended. All print orders issued hereunder are subject to the terms and conditions of the contract. The contract shall control in the event of conflict with any print order. A print order shall be "issued" upon notification by the Government for purposes of the contract when it is electronically transmitted or otherwise physically furnished to the contractor in conformance with the schedule.

REQUIREMENTS: This is a requirements contract for the items and the period specified herein. Delivery of items or performance of work shall be made only as authorized by orders issued under 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 above 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 because 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 delivery, the Government may procure this requirement from another source.

The Government may issue orders which provide for 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 under 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 l974 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.

IRS PRIVACY ACT CLAUSES: In conjunction with the Privacy Act of 1974, adherence to the following clauses are required:

Criminal Sanctions: 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 an agency, who by virtue of his/her employment of 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 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 $10,000.00.

Criminal/Civil Sanctions:

(a) Each officer or employee of any person at any tier to whom returns or return information is or may be disclosed shall be notified in writing by the person that returns or return information 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 such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure plus in the case of willful disclosure or a disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC Sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(b) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract and that inspection of any such returns or return information for a purpose or to an extent not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection of returns or return information 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 $1,000.00 for each act of unauthorized inspection with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection plus in the case of a willful inspection or an inspection which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRC Sections 7213A and 7431.

(c) 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 there under, 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.

Inspection:

The contractor shall be subject at the option/discretion of the ordering agency, to periodical testing (but no less than annually) and evaluation of the effectiveness of information security controls and techniques. The assessment of information security controls may be performed by an agency independent auditor, security team or Inspector General, and shall include testing of management, operational and technical controls, as indicated by the security plan or every information system that maintain, collect, operate or use federal information on behalf of the IRS. The IRS and contractor shall document and maintain a remedial action plan, also known as a Plan of Action and Milestones (POA&M) to address any deficiencies identified during the test and evaluation. The contractor must cost-effectively reduce information security risks to an acceptable level within the scope, terms and conditions of the contract. The contractor has the responsibility of ensuring that all identified weaknesses are either corrected and/or mitigated.

The Government shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, the Contracting Officer of the Washington GPO Office, may require specific measures in cases where the contractor is found to be noncompliant with contract safeguards.

Breach-Related Termination of Data Transmission:

If the Government determines that an authorized recipient has failed to maintain adequate safeguards (in the transmission, retention, and/or use of SBU) or has made any unauthorized inspections or disclosures of SBU, the Government may terminate or suspend transmission of SBU to any authorized recipient until the Government is satisfied that adequate steps have been taken to ensure adequate safeguards or prevent additional unauthorized inspections or disclosures (see I.R.C. § 6103(p)(4) and (p)(7)).

Sensitive But Unclassified Systems or Information:

(a) In addition to complying with any functional and technical security requirements set forth in the schedule and elsewhere in the contract, the contractor shall request that the Government initiate personnel screening checks and provide signed user nondisclosure agreements, as required by this clause, for each contractor employee requiring staff-like access, i.e., unescorted or unsupervised physical access or electronic access, to the following limited or controlled areas, systems, programs, and data: IRS facilities, information systems, security items and products, and sensitive but unclassified information. Examples of electronic access would include the ability to access records by a system or security administrator.

(b) The contractor shall submit a properly completed set of investigative request processing forms for each such employee in compliance with instructions to be furnished by the IRS.

(c) Depending upon the nature of the type of investigation necessary, it may take a period of up to eleven months to complete complex personnel screening investigations.

To verify the acceptability of a non-IRS, favorable investigation, the contractor shall submit the forms or information needed, according to instructions furnished by the IRS.

The contractor shall ensure that each contractor employee requiring access executes any nondisclosure agreements required by the Government prior to gaining staff-like access. The contractor shall provide signed copies of the agreements to the Contracting Officer's Representative for inclusion in the employee's security file. Unauthorized access is a violation of law and may be punishable under the provisions of Title 5 U.S.C. 552a, Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.)(governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)) and other applicable statutes.

NOTE: The contractor shall immediately notify the Contracting Officer (GPO) and the Contracting Officer's Representative of the termination, resignation, or reassignment of any authorized personnel under the contract. Further, the contractor shall include the steps taken to ensure continued performance in accordance with the contract. Replacement personnel or new hires must have qualifications that are equal to or higher than the qualifications of the person(s) to be replaced.

The contractor may contact Erika Bryant at erika.j.bryant@irs.gov, Sylvia Greene at sylvia.j.greene@irs.gov, and Brandis Dew Brandis.S.Dew@irs.gov regarding questions concerning requirements for a security clearance. The requirements include, but are not limited to, financial history of the contractor's firm and on-site visit(s) by the IRS security personnel.

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 before 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: Contractor's billing invoices must be approved before submitting to GPO for payment. Not later than five (5) workdays upon completion of each order, the contractor shall submit a PDF file of the itemized statement of billing to the Internal Revenue Services for verification, approval, and signature. The requisition number, program number, print order number, and survey form number shall be noted on the billing documents. Contractor to submit to the Internal Revenue Services to the email address indicated on the print order and cdominguezcastro@gpo.gov.

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

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

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

All contractor billing invoices must be itemized under the line items in the "SCHEDULE OF PRICES."

SECTION 2. – SPECIFICATIONS

SCOPE: These specifications cover the production of IRS Customer Satisfaction Survey Packets consisting of surveys, pre-notes, letters, postcards, and envelopes, requiring such operations as electronic prepress, printing, and variable imaging; binding, construction, package assembly, and distribution. Additionally, the contractor will be required to perform survey administration tasks such as managing multiple surveys in varying stages, monitoring ID numbers, and accepting existing (and future) surveys in a press-quality PDF format.

TITLE: Customer Satisfaction Survey Packets.

CONTRACT DATA FILE REQUIREMENTS SUMMARY AND OVERVIEW:

Incoming Data/Preparation: Each month, the MRF will furnish the contractor with a file containing names and addresses of selected taxpayers (and other variables) targeted to receive a survey. Upon receipt, the contractor will check the integrity of the data contained in the file to ensure that there are no duplications and that all information is in the proper field and send an email to the publishing specialists and MRF confirming data integrity in timely manner (within three (3) hours of receipt of data file), as follows: "Data received. Counts verified. Formatting verified." Addresses will be in Zip Code sequence and not truncated. Files will be in MS Excel format. The zip code column should be formatted as general or text, not numeric or custom "zip code." Contractor must be able to receive and utilize data that is furnished in various formats, for example, 9-digit zip, 5+4 zip.

In addition to the names and addresses, the data set will include a unique ID associated with each taxpayer. That unique ID must be converted to a standard barcode format so that when surveys are received by the MRF, they can match respondents against the master file. The contractor may use, at their option, a second barcode, or whatever means necessary, to ensure consistency among components throughout the process. One hundred percent accuracy is required when matching letters and surveys for Waves 2 and 4.

It is the responsibility of the contractor to monitor all ID numbers to ensure that the unique number assigned to the individual selected taxpayer follows that selected taxpayer on all correspondence from start to finish of that survey process.

The contractor must create a barcode, readable on their equipment, that is associated with the unique ID number overprinted onto each survey. Once assigned, this number must be reproduced on all applicable documents associated with that unique taxpayer (i.e., pre-notification letter, survey, postcard).

When the unique ID number is in barcode format, it should appear in 3 of 9 barcode font. When the unique ID number is human readable, it must be in Arial font with a minimum font size of 10. The barcode must consist of the unique ID number followed by the year and month corresponding to the closed case month. For example: 201301 for January 2013; 201302 for February 2013.

Contract Closeout: All information must be purged from the contractor's system within 30 calendar days of contract expiration.

SURVEY PACKET ITEMS: Upon award, the contractor will be supplied electronic files of all existing survey forms in press-quality PDF format with all fonts embedded. Surveys must be performed on the scanning equipment utilized to gather data received from the selected taxpayers.

- Surveys (two-page survey or four-page survey).
- Pre-notification letters (hereinafter referred to as "Pre-note", printed on Government furnished official IRS letterhead stationery).
- Letters.
- Postcards (standard or folded postcard).
- No.9 Business Reply Envelope (BRE).
- No.10 Window Envelope (mailing envelope).

Print order will specify which letterhead (pre-notes only) and envelope to use.

A typical mailing schedule for one month's receipt of data per unique survey is in four (4) mailing waves as follows:

Wave 1: Pre-note mailed to each recipient using a mailing envelope.

Wave 2: Initial Survey Packet #1 consisting of:

- Letter 1
- Survey
- BRE
- Mailing Envelope

Wave 3: Postcard to encourage and remind taxpayer to respond.

Wave 4: Non-respondent Survey Packet #2 consisting of:

- Letter 2
- Survey
- BRE
- Mailing Envelope

NOTE: The majority of the surveys will have four (4) waves. An occasional 5th wave may be added with any combination of components. There are a few exceptions that require mailing Waves 1 through 3 in the 3rd month of each quarter with no 4th wave. Two (2) surveys require mailing only the pre-note letter on a quarterly basis. However, there are surveys throughout the year that will require unique schedules with varying mailing waves (see Exhibit B for example of schedules). Contractor must mail per the instructions provided with the individual print order.

FREQUENCY OF ORDERS: Approximately 170 to 300 orders per year.

NOTE: Several orders will run concurrently throughout the month/quarter. Usually, a print order will be issued each month of the quarter for each survey for a total of three (3) print orders per quarter/per unique survey; however, occasionally due to a specific requirement, the Government may issue one (1) print order to cover all of the monthly requirements for a particular survey.

During the term of the contract, there may be times when one month (usually the first in a new fiscal year) will be combined with the following month, causing the number of print orders issued to double. While two months of data will follow the same schedule, the number of print orders for each full quarter is usually three (3) (for a 6-month collection, there will be six (6)). For the surveys sending only pre-notes, the number of print orders placed will vary each quarter. The number of print orders placed correlates with the number of data sets pulled monthly by the Government and sent to the MRF. NOTE: There is a possibility this will occur for the first quarter of the contract.

There are a total of 21 surveys. The mailing schedule to use will be indicated on the print order per the "SCHEDULE."

During the term of this contract, additional surveys may be required and will be generated as needed. The contractor will work closely with the IRS, as well as the MRF, to implement the new surveys as they are required. All terms and conditions in these specifications will apply to any future surveys.

QUANTITY:

Survey 1: Up to approximately 7,500 copies per order.

Survey 2: Up to approximately 7,500 copies per order. (Survey 2 is only sent to the non-respondents of Survey 1. Based on historical data, the non-respondent rate is approximately 85%.)

Pre-Notes: Up to approximately 7,500 copies per order.

Letters: Up to approximately 7,500 copies per letter per order.

Postcards: Up to approximately 7,500 copies per order.

An occasional order may be placed for up to approximately 11,000 copies on any order with any item combination.

The print order issued each month for a unique survey will reflect the requirements for the 1st, 2nd, and 3rd mailing waves. The quantity for the 4th mailing wave is contingent on the responses.

NOTE: The majority of print orders will be for approximately 1,500 copies or less.

NUMBER OF PAGES:

Surveys: At this time, there are two (2) different styles of surveys:

Two-Page Survey: Face and back.

Four-Page Survey: Face and back.

Pre-Notes and Letters: Face only.

Standard and Folded Postcards: Face and back.

Envelopes: Face only (after construction).

TRIM SIZE:

Two-Page Survey: 8-1/2 x 11".

Four-Page Survey: 17 x 11" flat (folded down to 8-1/2 x 11").

Pre-Notes and Letters: 8-1/2 x 11".

Standard Postcards: 5-1/2 x 4-1/8".

Folded Postcards: 8-1/2 x 11" flat (folded down to 8-1/2 x 5-1/2").

Business Reply Envelope (BRE): No. 9 (3-7/8 x 8-7/8"), plus flap.

Mailing Envelope: No. 10 window envelope (4-1/8 x 9-1/2"), plus flap.

GOVERNMENT TO FURNISH: Data files with taxpayer information specific to the survey/pre-notes/letters/envelopes/postcards will be furnished with each print order. (See "CONTRACT DATA FILE REQUIREMENTS SUMMARY AND OVERVIEW.")

Existing Surveys: Upon award, press-quality PDF files of the current surveys being used will be furnished for the static matter. These files must be held for use throughout the term of the contract. PDFs of revised surveys, postcards, envelopes, and letters will be provided as needed.

Future Surveys: Government will furnish electronic media (see below) for future surveys when required, to be furnished as follows:.

Platform:	Microsoft Windows (current or near current version).
Storage Media:	Email; Secure File Transfer Protocol (SFTP). The data files for the mailing addresses will be furnished to the contractor from the MRF via contractor's hosted SFTP.
Software:	Static Matter: Adobe Acrobat (current or near current version); Variable Data: Microsoft Excel, SecureZip™. (Current or near-current versions will be used for Microsoft Excel and SecureZip™.) NOTE: All Government software upgrades (for specified applications) which may occur during the term of the contract must be supported by the contractor.
Fonts:	All printer and screen fonts will be embedded. The contractor is cautioned that furnished fonts are the property of the Government and/or its originator. 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 native application and/or PDF format.

Upon award, the contractor will be supplied electronic files of all existing survey forms in press-quality PDF format with all fonts embedded. (See "SURVEY PACKET ITEMS".)

Preprinted IRS Letterhead (White 25% Cotton Bond, basis weight: 20 lbs. per 500 sheets, 17 x 22", equal to JCP Code G45) will be furnished for all pre-notes. The letterhead is produced via offset printing, and the ink used on the furnished letterhead will not smear when used on the contractor's equipment.

Unique Letterheads (Pre-notes): Will use approximately six (6) unique letterheads. Contractor must use the letterhead as specified on the print order. Additional unique letterheads may be required.

Current Letterhead Form numbers and corresponding IRS Business Unit:

Form 13014 – Appeals
Form 13038 – Small Business/Self-Employed (SB/SE)
Form 13040 – Wage & Investment (W&I)
Form 13042 – Large Business & International (LB&I)
Form 13044 – Tax Exempt & Government Entities (TE/GE)
Form 13081-A – Taxpayer Advocate Service (TAS)

Files to Initiate Customer Satisfaction Survey Process: Initial data files from the MRF will be submitted in the aforementioned software programs (see "CONTRACT DATA FILE REQUIREMENTS SUMMARY AND OVERVIEW, *Incoming Data/Preparation*").

Dummy data files and record layout to be used for the proofs will be emailed to the contractor one (1) workday after award. NOTE: Dummy data files do not get processed through NCOA.

One copy of IRS Form 13456 (IRS Publishing – Postage Report) will be furnished, via email, in a fillable PDF file format.

Identification markings such as register marks, commercial identification marks of any kind, etc., carried in the electronic files, must not print on finished product.

EXHIBITS: The samples pages shown as Exhibits A, B, D, E, and F are representative of the requirements which will be ordered under this contract. However, it cannot be guaranteed that future orders will correspond exactly to these exhibits.

Exhibit A – Typical Surveys
Exhibit B – Typical Schedules
Exhibit C – Form 13456 and Postage Statement Exhibit
Exhibit D – Typical Pre-Notes
Exhibit E – Typical Letters
Exhibit F – Typical Postcard
Exhibit G – Form 14573 Survey Checklist of Scanned Mail Component
Exhibit H – Form 14604 Contractor Separation Checklist
Exhibit I – IRM Exhibit 10.8.2-1 (09-30-2016) Roles that Require Specialized Training
Exhibit J – Website Links
Exhibit K – Proofs, and Prior-to-Production Samples Distribution
Exhibit L – Physical Security Self-Assessment
Exhibit M – Cyber Security Self-Assessment

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

Contractor is responsible for setting up and maintaining a secure network according to the National Institute of Standard and Technology (NIST) SP 800-53 security guidelines. Prior to award, the contractor will be required to submit in writing to GPO that the contractor is able to meet this requirement. Passwords for the encrypted SecureZip™ files will be supplied through secure data transfer (SDT).

Contractor MUST be capable of processing all requirements for each survey as required throughout the term of this contract. Orders will run concurrently, and many processes will overlap. Exhibit B is representative of the schedule requirements under the contract.

NOTE: Occasionally, due to the needs of the Government, the contractor may be handling two or more data files months for processing in the same calendar month with all of the processes running concurrently.

The contractor must have Internet access provided through their Internet Service Provider (ISP), an email account, and a web browser.

The contractor must furnish an email address for the IRS to email the forms mentioned above. NOTE: The use of public address or web-based mail servers (ex: Hotmail, Yahoo, Juno) are not permitted.

NOTE: Some programming may be required by the contractor on new and/or existing surveys.

IRS-Furnished Letterhead Stock: The contractor will be required to store the furnished stock in a manner that provides protection from any type of damage, especially from the elements.

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 furnished material and notifying the Government of any shortage within 24 hours of receipt thereof.

Responsibility for Inspections and Tests: The contractor is responsible for any inspections and tests required to ensure that the supplies provided under the contract conform to the specifications and contract requirements listed herein. The right of the Government to perform inspections and tests does not relieve the contractor from this responsibility. Inspections shall be made by the contractor of a representative sample of finished items to determine compliance with specifications. The sampling and inspections may be performed during the course of the production run. Contractor must develop and submit prior to award a quality control checklist for all components of the survey production process. (See "PREAWARD PLANS".)

Contractor's Records: The contractor shall maintain records of all inspections and tests performed on the supplies provided under the contract. The contractor shall save and preserve all records of these inspections and tests for a minimum of 90 calendar days after delivery, or until they are released by the Government. The contractor will make all records of these inspections and tests available for inspection by the Government.

DOMAIN NAME AND SSL CERTIFICATE: The contractor's application will be protected using Secure Socket Layer (SSL), or equal, technology which is a protocol for transmitting private documents via the Internet. Both Netscape Navigator and Microsoft Edge support SSL and many websites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "*https:"* instead of "*http:*".

In a coordinated effort to meet the survey requirements of the IRS, the contractor will be required to interact closely with the IRS and one or more Marketing Research Firms (MRF). (NOTE: Hereinafter whenever MRF is referenced, it is understood that the contractor will be receiving files from the MRF). Further, it is the responsibility of the contractor to put safeguards in place that will distinguish between files generated by each MRF to ensure that there is no possibility of inter-mixing data/files/etc.

The contractor must appoint someone at their company to serve as the Project Manager to oversee the operation from beginning to end. The name and phone numbers of the Project Manager and their core team will be furnished to GPO and the IRS.

Conferences for each survey project may require more contact initially. Where appropriate, teleconferences with all involved parties may be held in lieu of face-to-face meetings. An overview of the expectations and goals of the project will be shared. There will be an opportunity for the contractor to obtain clarification and project-specific information as needed to fulfill the goals of the project. Discussions include, but are not limited to, such issues as file layout, preferred format of sample, and target timeframes.

ELECTRONIC PREPRESS: Immediately upon receipt of Government-furnished material and prior to image processing, the contractor shall perform an in-depth preflight check of the furnished media and publishing files to ensure the correct output of the required reproduction image. This preflight check is to include accurate identification of all fonts used and/or missing fonts, identification of colors used within the file, and any errors, media damage, or data corruption that might interfere with proper file image processing. NOTE: All problems with furnished media must be reported within three (3) hours of receipt to the ordering agency and the GPO contract specialist.

With the agency's approval, the contractor may 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 output must be 150-line screen or finer for all screens and a minimum of 2400 dpi for the remainder.

When required by the Government, the contractor shall make minor revisions to the electronic files. It is anticipated that the Government will make all major revisions.

Prior to making revisions, the contractor shall copy the furnished files and make all changes to the copy.

Upon completion of each order, the contractor must furnish final production native application files with the furnished material. The digital deliverables must be an exact representation of the final printed product and shall be returned on the same type of storage media as was originally furnished. The Government will not accept, as digital deliverables, PostScript files, Adobe Acrobat Portable Document Format (PDF) files, or any proprietary file formats other than those supplied, unless specified by the Government. NOTE: The Government will accept PDF files as digital deliverables when furnished by the Government.

PROOFS: The proof requirements as specified below are required on the first order and at any time during the term of the contract when a new component is added, or a current component is revised.

The proofs as specified below will be required for each unique survey and must be sent according to the specified recipients as indicated in Exhibit K. Complete addresses will be provided after award.

PDF Proofs: 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. Proofs must show all margins. Proofs will be transferred to the agency via SFTP.

NOTE: Proofs for envelopes must show all margins and dimensions, indicate trim marks, show flap, and show size/placement of the window.

If contractor is producing the requirements via offset printing:

Digital Color Content Proofs: 10 sets of all survey components (including envelopes). 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.

Digital color content proofs must utilize Government-furnished “dummy data” which consists of 10 addresses. Proofs must include all variable data that will print on the final product.

If contractor is producing the requirements via digital printing:

Digital One-Off Proofs: 10 sets of all survey components (including envelopes) created using the same output device that will be used to produce the final printed product on the actual production stock. Proofs shall be collated with all elements in proper position (not pasted up), imaged face and back, trimmed, and folded to the finished size/format of the product, as applicable. Proof will be used for color match on the press on the production run.

Digital one-off proofs must utilize Government-furnished “dummy data” which consists of 10 addresses. Proofs must include all variable data that will be printed on the final product.

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

Contractor must not print prior to the receipt of an “O.K. to Print.”

PRIOR-TO-PRODUCTION SAMPLES: The prior-to-production samples as specified below are required on the first order and at any time during the term of the contract when a new component is added, or a current component is revised.

Prior to the commencement of production of the contract production quantity, 10 sample sets of the complete survey packet consisting of each component (including No. 9 and No. 10 envelopes) are required for each wave of each survey. The container and accompanying documentation shall be marked "PRIOR-TO-PRODUCTION SAMPLES" and shall include the GPO Purchase Order, Jacket, Program, and Print Order numbers.

Each component shall be printed, bound/constructed (as applicable), and assembled as specified and must be of the size, kind, and quality that the contractor will furnish. All components must be printed on the stock specified herein, as applicable to each component. NOTE: The No. 10 envelope samples do not require the die-cut window; however, the samples must clearly indicate the size and position of the envelope window.

Samples will be inspected and tested for conformance of materials and must comply with the specifications as to construction, kind, and quality of materials.

Samples must utilize Government-furnished "dummy data" which consists of 10 addresses. Samples must include all variable data that will be printed on the final products.

NOTE: All surveys must be compatible for scanning on an Insight 70, Scantron Insight 700c, Fujitsu FI-5950, Fujitsu FI-7160, and Fujitsu fi-6800.

Samples will be required for each unique survey and must be sent according to the specified recipients as indicated in Exhibit K. Complete addresses will be provided after award.

The contractor must submit all required samples within three (3) workdays of receipt of approval of digital color content proofs.

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

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

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

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

Manufacture of the final product prior to approval of the samples submitted is at the contractor's risk. Samples will not be returned to the contractor. All costs, including the costs of all samples, shall be included in the contract price for the production quantity.

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

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

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

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

Surveys and Letters: White No. 1 Smooth-Finish Text, basis weight: 60 lbs. per 500 sheets, 25 x 38", equal to JCP Code A61.

Pre-Notes: The stock for the pre-notes (for all surveys) will be provided by the IRS for each specific official letterhead for business units. It is the responsibility of the contractor to maintain three (3) months' inventory of the letterhead. When reordering the letterhead, the contractor must notify the IRS within two (2) weeks prior to the delivery of stock.

Standard and Folded Postcards: White Index, basis weight: 110 lbs. per 500 sheets, 25-1/2 x 30-1/2", equal to JCP Code K10.

Envelopes: White Writing Envelope, basis weight: 24 lbs. per 500 sheets, 17 x 22", equal to JCP Code V20.

PRINTING AND VARIABLE IMAGING: The Government reserves the right to make changes to any item at any time during the term of the contract. Therefore, stockpiling is at the contractor's risk. The Government shall not be required to purchase from the contractor the surplus/inventory of any items on hand in excess of what was ordered on a print order.

At contractor's option, the products may be produced via conventional offset or digital printing provided Quality Level III standards are maintained. Final output must be a minimum of 150- line screen and at a minimum resolution of 1200 x 1200 dpi x 1 bit or 600 x 600 dpi x 4-bit depth technology. Digital device must have a RIP that provides an option for high quality color matching such as Device Links Technology and/or ICC Profiles. NOTE: Contractor must produce the entire job either conventional offset or digital printing; split production methods are not acceptable without prior approval.

NOTE: The GPO imprint must not print on any of the components.

Surveys: Match Pantone number as indicated on the print order.

Two-page Surveys: Category 1: Print face and back in black ink only. Printing may consist of type, rule matter, bubbles/boxes, hash/tick marks, or other marks unique to the scanning equipment to be used, screens, and line art. Image variable data in black on the face only. Imaging consists of a unique human-readable ID and corresponding barcode. (NOTE: 15 of the existing surveys are in Category 1.)

Category 2: Print face and back in black and one (1) Pantone ink color. Printing may consist of type, rule matter, bubbles/boxes, hash/tick marks, or other marks unique to the scanning equipment to be used, screens, and line art. Image variable data in black on the face only. Imaging consists of a unique human-readable ID and corresponding barcode. (NOTE: 2 of the existing surveys are in Category 2.)

Four-page Surveys: Print face and back in black and one (1) Pantone ink color. Printing may consist of type, rule matter, bubbles/boxes, hash/tick marks, or other marks unique to the scanning equipment to be used, screens, and line art. Image variable data in black ink on the first page of the survey. Imaging consisting of a unique human-readable ID and corresponding barcode.

Extraneous marks, hickies, and/or spots in the answer boxes are not acceptable.

Laser-safe ink is required to withstand laser-processing heat on forms that require subsequent laser slugging and identification. These inks must meet the specifications of laser printer manufacturers and must be tested by the contractor.

Contractor must have a post-production quality control checklist to include fanning all offset printed stock to verify that only correct stock is used to avoid overprinting on the incorrect offset stock when surveys are printed consecutively.

All surveys must be compatible for scanning on an Insight 70, Scantron Insight 700c, Fujitsu FI-5950, Fujitsu FI-7160 and Fujitsu fi-6800.

Pre-Notes and Letters: Print face only in black ink. Printing consists of static text matter. Image variable data in black on the face only. Imaging consists of date, unique human-readable ID and corresponding barcode, respondent's name, address, password, and PIN number.

Postcards: Print face and back in black ink only. Printing consists of static text matter. Image variable data in black on the face only. Imaging consists of a unique human-readable ID and corresponding barcode, respondent's name, address, and PIN number.

No. 9 and No. 10 Envelopes: Print face only (after construction) in black ink or in one (1) Pantone ink color. Match Pantone number as indicated on the print order.

Printing of all envelopes shall be in accordance with the requirements for the envelope style ordered. All printing shall comply with all applicable U.S. Postal Service regulations, including automation guidelines/requirements. The envelope shall accept printing without feathering or penetrating to the reverse side.

At present, there are 11 unique No. 10 mailing envelopes and six (6) unique No. 9 business reply envelopes. The number of unique envelopes is subject to change at any time.

MARGINS: Adequate gripper. Margins will be as indicated on the print order or furnished electronic files. No bleeds.

BINDING:

Surveys:

Two-Page Survey: Trim four sides.

Four-Page Survey: Fold from 17 x 11" down to 8-1/2 x 11", first page out. Trim three sides.

Pre-Notes and Letters: Trim four sides.

Standard Postcard: Trim four sides.

Folded Postcard: Fold from 8-1/2 x 11" down to 8-1/2 x 5-1/2", mailing address out. Trim three sides. At contractor's option, tab, wafer seal, or glue strip per USPS regulations for self-mailing.

CONSTRUCTION (Envelopes):

No. 9 Business Reply Envelope (3-7/8 x 8-7/8"): Envelope must be open side, side or diagonal seams, at contractor's option, with water-soluble gummed, fold-over flap for sealing. Flap depth is at the contractor's option but must meet all USPS requirements. Flap adhesive must not adhere to the contents of the envelope.

No. 10 Mailing Envelope (4-1/8 x 9-1/2"): Envelope must be open side, side or diagonal seams at contractor's option, with water-soluble gummed, fold-over flap for sealing. Flap depth is at the contractor's option, but must meet all USPS requirements. Flap adhesive must securely seal the envelope without adhering to contents, permit easy opening by the recipient, and not permit resealing of the envelope.

Face of No. 10 envelope to contain a 1-5/8 x 4-1/2" die-cut address window with slightly rounded comers. Die-cut window is to be located 1/2" from the bottom edge of the envelope and 3/4" from the left edge of the envelope (the long dimension of the window is to be parallel to the long dimension of the envelope). The contractor has the option to adjust the size of the window opening (subject to Government approval), providing the visibility of the mailing address and intelligent mail barcode on the pre-note and the explanation letter is not obscured, and other extraneous information is not visible when material is inserted into the envelope. Window is to be covered with a suitable, transparent, low-gloss poly-type material that must be clear of smudges, lines, and distortions. Poly-type material must be securely affixed to the inside of the envelope so as not to interfere with the insertion of contents. Window material must meet the current U.S. Postal Service's readability standards/requirements.

PACKAGE ASSEMBLY:

Surveys and Letters:

Surveys: Fold survey from 8-1/2 x 11" to 8-1/2 x 3-2/3" using two (2) parallel folds.

Letters: Fold letter from 8-1/2 x 11" to 8-1/2 x 3-2/3" using two (2) parallel folds, address out.

Insert folded letter, followed by folded survey, (on a machine equipped with a camera system) with one (1) business reply envelope (for Survey 1 and Survey 2 mailing waves) into the mailing envelope with recipient's name/address and barcode facing out for visibility through window envelope and seal the mailing envelope.

NOTE: Cameras are to be used on letters and surveys to ensure the piece matching ID (printed in the upper right corner of both) is the same on both the letter and the survey as they are being inserted.

It is the contractor's responsibility to ensure that only one letter, one survey, and one business reply envelope are inserted into the specified mailing envelope. Contractor must perform the "tap test" to ensure that nothing but the address and IMb barcode on the letter is visible through the window.

Pre-Notes: Fold from 8-1/2 x 11" to 8-1/2 x 3-2/3" using two parallel folds, address out. Insert one pre-note letter into the mailing envelope and seal.

It is the contractor's responsibility to assure that only one pre-note letter is inserted into the mailing envelope, and that only the mailing address and postal barcode on the pre-note is visible through the window. Contractor must perform the "tap test" to ensure that nothing but the unique human-readable ID, respondent's name, address, and IMb barcode appear in the window.

QUALITY ASSURANCE RANDOM COPIES: 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 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: Mail f.o.b. contractor's city.

Complete addresses and quantities will be furnished with each print order.

All mailing shall be made at the First-Class rate.

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

National Change of Address (NCOA) Link Processing, LACSLink, and Delivery Point Validation (DPV): Contractor is responsible for taking the IRS raw data files (with the exception of those furnished for proof purposes and specified mailings, as indicated on the print order) and passing the files against the NCOALink, LACSLink, and DPV file using a licensed USPS Full-Service Provider.

Contractor must select the new move addresses from the mail file, verify the service center code of the new move addresses, make all necessary service center code corrections using the furnished electronic file, and merge the new move addresses back into the mail file. Any addresses that are determined to be undeliverable must be pulled from the mail file.

Any undeliverable must be furnished to the Marketing Research firm and the IRS representative within 24 hours. All NCOA update files should be an Excel spreadsheet with the following variables: Unique ID and CASS error code.

There will also be certain surveys in which the addresses have been verified by the IRS (confirmed by current correspondence to the recipient) that have more accurate/current addresses than are on the database from the USPS. These surveys will be designated as "do not use NCOA Link, Accumail, or any other postal verification."

NOTE: If the file is furnished as a comma-delimited file, contractor will be required to manipulate the file in order for the zero to print. Files saved in a comma-delimited format do not allow for leading zeros in a zip code.

Mailing Requirements: Mail must be Presorted to maximize postal discount to USPS First Class Letter Commercial Automation 5-digit and AADC levels whenever possible.

NOTE: The contractor must supply a local USPS contact name and number at the time of award so that the permit process can be expedited.

Orders which result in mailings of less than 200 pieces or less than 50 pounds will require the contractor to apply the appropriate postage to each mailing. Contractor will be reimbursed for postage by submitting a properly completed Postal Service Form with billing invoice for payment. If an approved USPS Seamless Acceptance Mailer for mailings under 200 pieces contractor may utilize the appropriate USPS Mailing Statement (e.g. PS 3602) using the provided "Postage and Fees Paid" Indicia. Upon completion of each print order, contractor must follow the guidelines for submitting Form 13456.

NOTE: Postage must be metered or printed. Stamps are not acceptable. Metering must not extend past the edge of the postcard or envelope; when using metered tab, tab should not lift off causing a ragged edge when sent through USPS equipment. Contractor is responsible for the meter and all meter supplies.

All copies mailed must conform to the appropriate regulations in the U.S. Postal Service manuals for "Domestic Mail" or "International Mail," as applicable.

The contractor must comply with all U.S. Postal Service regulations governing the preparation of First-Class rate mailings which are in effect at the time of the mailing for both domestic and international mail, including the issuance of the required forms (mailing statements) and the weighing of shipments. The contractor must meet with local postal authorities before the start of production.

The Domestic Mail Manual (DMM) has specific requirements regarding the minimum and maximum package sizes the contractor must adhere to.

Intelligent Mail Barcode (IMb): Contractor will be required to create and apply the proper USPS IMb coding for tracking purposes for billing and research for the IRS.

Contractor will utilize the USPS Informed Visibility (IV) Mail Tracking & Reporting (IV-MTR) service that provides end-to-end mail tracking information for letter and flat pieces, bundles, handling units, and containers. Contractor will provide mail-scanned events reports or provide access to the reports that include, at a minimum: mail drop date, quantities, postage, and last delivery scan event. If requested for the contractor to provide reports, the reports will be made available by close of business Friday for the week in which a mailing has occurred. Contractor must adhere to all USPS Domestic Mail Manual and USPS IV Mail Tracking and Reporting Guide requirements. Contractor may not charge additional fees for providing reports.

Contractor to furnish documentation on 100% of mail turnover to USPS by the date specified on the print order.

USPS Secure Destruction: If requested contractor must implement Secure Destruction which is a value-added USPS service that securely shreds undeliverable mail instead of returning to the sender and providing electronic notification of mail designated for destruction. If instructed, contractor will use IRS provided designated Mailer ID and USPS Service Type Indicator (STID) for USPS Secure Destruction. Contractor must include provided Mailer ID and STID within the Intelligent Mail Barcode.

If the contractor is allowed to use contractor Mailer ID, contractor must sort daily Secure Destruction data records and segment them by each mailing job. The contractor must compile the daily data received into a report to send to the IRS weekly that comprises the prior week's results. Contractor may not charge additional fees for providing reports.

USPS Informed Delivery: If directed the contractor must implement Informed Delivery using the IRS provided Mailer ID. Contractor must set up the mailing file (eDoc) to include the MID, identify the mail owner and mail preparer in the "By/For" fields by CRID, MID or permit number and include the Informed Delivery discount code.

Contractor must register an IRS mailing indicia with the entry post office to ensure the best rate for mailing. Mailing must conform to all U.S. Postal Service regulations with regard to bulk mail. A signed Postal Service Form 3600-R and Postal Service Form 3607-R reflecting the cost for each mailing wave for each print order (usually four separate mailing waves per order) must be submitted with the contractor's billing invoice reflecting the requisition number, program number, print order number, survey form number, and wave number.

Upon completion of each print order:

- Contractor must complete and submit via email Form 13456 (in a PDF file) to the IRS within three (3) workdays after each turnover of the product to the USPS. Details to fill in the data fields, rename the PDF, and email are on the second page of the furnished form. Scanned pages of the Form 13456 will not be accepted. Any delay or missing input could result in delay of payment.

- Contractor must capture the following fields from every postage statement (e.g. USPS Form 3602):
  - Name of contractor
  - Contact person at contractor's office
  - Telephone number of contact person
  - Email address of contact person
  - Mailing start date: The date the first piece is mailed
  - Mailing end date: If not all pieces were sent on the start date, this is the date the last piece is mailed.
  - Mailings: (Optional). Check this box to note there will be multiple mailings
  - Wave: Check this box to note that the multiple mailings will be sent in "waves." Use the blank fields next to this check box to distinguish the number of current wave from the number of total waves.
  - Zip Code: The zip code of the post office from which pieces are mailed

  - Date on Mailing Statement: The mailing date on the postage statement
  - Pieces Mailed: The number of envelopes, containers, etc., that is mailed
  - Copies Mailed: The total number of items inside each envelope, container, etc., that is mailed
  - Postage Amount: The total dollar amount listed on each postage statement
  - Postage Statement Type: Use the pull-down menu to designate which type of postage statement (i.e., USPS Form 3602, 3602-R, 3605, 3600, 3607R) was used.

- Form 13456 must contain only postage information for the IRS requisition number at the top of the form. Contractor must not combine postage associated with multiple print order/requisition numbers on a single form.

- If all the lines on the front of Form 13456 are filled in, use the "Add New Mailing" button to add another row of data.

NOTE: Any delay or missed input with either of the forms could result in delay of payment.

Upon completion of each order, the contractor must notify the ordering agency (on the same day the order mails, not later than 1:00 pm EST) via email to the address indicated on the print order. The subject line of the email shall be "Distribution Notice for Program 837-S, Print Order XXXXX, Jacket Number XXX-XXX." The notice must provide all applicable tracking numbers, mailing method, and title of the product. Contractor must be able to provide copies of all mailing receipts upon agency request.

Within three (3) workdays of completion of the mailing, contractor must furnish a copy of the completed Post Service Form 3600-R and Postal Service Form 3607-R to the following address (via GROUND utilizing the IRS small carrier account): IRS, Attn: Sylvia Greene, 250 Georgia Avenue, E., #1658, Fayetteville, GA 30214-9998. Further, contractor MUST update IRS Electronic Form 13456 per instructions on Page 2 of Form 13456.

Upon completion of the contract, contractor must return/deliver the balance of any unused furnished stock to one address as instructed by the ordering agency.

Within 120 calendar days of completion of each order, all Government furnished materials (except those ordered held for future use) must be permanently deleted from the contractor's network. Information must not be recoverable. Contractor is required to keep a log capturing file name and date of deletion.

All expenses incidental to picking up and returning furnished material, submitting proofs and prior-to-production samples, and furnishing sample copies must be borne by the contractor.

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

Print order and furnish materials will be sent via email.

PDF soft proofs must be emailed to the ordering agency at the email address indicated on the print order.

Hard copy proofs and prior-to-production samples must be delivered as indicated on Exhibit K. Complete addresses will be provided after award.

No definite schedule for placement of orders can be predetermined.

NOTE: Occasionally, due to the needs of the Government, the contractor may be handling two (2) or more data month files for processing in the same calendar month with all the processes running concurrently.

The following schedules begin upon receipt of data set, verification of counts, and formatting (see "CONTRACT DATA FILE REQUIREMENTS SUMMARY AND OVERVIEW, *Incoming Data/Preparation*").

The numbers under the column headed "WD After" represent the number of workdays allowed to complete that certain part of the schedule.

Proofing and Construction/Prior-to-Production Sample Schedule:	WD After
Contractor to submit PDF proofs	3
Agency to return PDF proofs to contractor	2
Contractor to submit content proofs	2
Agency to return content proofs to contractor	2
Contractor to submit prior-to-production samples	3
Agency to return prior-to-production samples	2

The following schedules begin after receipt and approval of samples:

SB/SE and W&I Schedules:	WD After
Contractor to mail Pre-Notes	5
Contractor to mail Survey Packet #1	3
Contractor to mail Postcards	5
Contractor to mail Survey Packet #2	10

LB&I, TE/GE, and TAS, Schedules:	WD After
Contractor to mail Pre-Notes	5
Contractor to mail Survey Packet #1	3
Contractor to mail Postcard #1	5
Contractor to mail Survey Packet #2	15
Contractor to mail Postcard #2	15

SB/SE, LB&I, and TAS Schedules:	WD After
Contractor to mail Pre-Notes	10
Contractor to mail Survey Packet #1	5
Contractor to mail Postcards	5
Contractor to mail Survey Packet #2	15

LB&I, Survey Form Schedules:	WD After
Contractor to mail Pre-Notes	5
Contractor to mail Letter #1	3
Contractor to mail Postcard #1	5
Contractor to mail Letter #2	15
* Contractor to mail Letter #2	15

LB&I Alternative Schedule #1:	WD After
Contractor to mail Pre-Notes	5
Contractor to mail Letter #1	3
Contractor to mail Postcard #1	10
Contractor to mail Letter #2	10
* Contractor to mail Letter #3	10

LB&I Alternative Schedule #2:	WD After
Contractor to mail Pre-Notes	5
Contractor to mail Letter #1	3
Contractor to mail Postcard #1	15
* Contractor to mail Postcard #1	15
* Contractor to mail Letter #2	15

TAS QR Code Survey Schedule:	WD After
Contractor to mail Postcard #1	10
Contractor to mail Survey Packet #1	15
Contractor to mail Postcards #2	10
Contractor to mail Survey Packet #2	20

Appeals Schedule:	WD After
Contractor to mail Pre-Notes	5

** These are optional waves and will be added to that schedule when indicated on the print order.*

The ship/deliver date indicated on the print order is the date products ordered for mailing f.o.b. contractor's city must be delivered to the U.S. Postal Service.

Unscheduled material such as shipping documents, receipts or instructions, delivery lists, 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 Offices 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.

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."

I.	(a)	80
	(b)	80
	(c)	80
II.	(a)	431,758
	(b)	24,926
	(c)	73,751
	(d)	252,834
	(e)	539,794
	(f)	272,489
	(g)	98,237
	(h)	526,472
	(i)	799,298
III.		23

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 100 will be prorated at the per-100 rate.

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

I. ELECTRONIC PREPRESS: The prices offered shall include the cost of all required materials and operations, in accordance with these specifications.

(a) PDF proof.....per file.....$_____

(b) Digital color content or Digital one-off proofs.....per trim/page-size unit.....$_____

(c) Prior-to-production samples.....per trim/page-size unit.....$_____

II. PRINTING/VARIABLE IMAGING, BINDING, CONSTRUCTION, PACKAGE ASSEMBLY, AND DISTRIBUTION: Prices offered shall include the cost of all required materials and operations (including paper) necessary for the static and variable image printing, binding, construction, package assembly, and distribution of the products listed in accordance with these specifications.

Prices submitted must include the cost of collating, folding, and inserting the various components into the mailing envelopes, as applicable.

NOTE: Contractor is not allowed to charge for paper furnished by the Government.

	Running Per 100 Copies
(a) Two-Page Survey (8-1/2 x 11"): Category 1: Printing face and back in black ink and imaging face only in black ink, including binding.....per survey	$_____

_____
(Initials)

Running Per
100 Copies

(b) Two-Page Survey (8-1/2 x 11"): Category 2:
Printing face and back in black ink and one Pantone
ink color and imaging face only in black ink, including binding ..... per survey ..... $_____

(c) Four-Page Survey (17 x 11"):
Printing face and back in black ink and one Pantone
ink color and imaging on first page in black ink, including binding ..... per survey ..... $_____

(d) Pre-Note (8-1/2 x 11") (Government Stock):
Printing face only in black ink and imaging
face only in black ink, including binding ..... per pre-note ..... $_____

(e) Letter (8-1/2 x 11"):
Printing face only in black ink and imaging
face only in black ink, including binding ..... per letter ..... $_____

(f) Standard Postcard (5-1/2 x 4-1/8"):
Printing face and back in black ink and imaging
face only in black ink, including binding ..... per postcard ..... $_____

(g) Folded Postcard (8-1/2 x 11" flat):
Printing face and back in black ink and imaging
face only in black ink, including binding ..... per postcard ..... $_____

(h) Business Reply Envelope (No.9)
Printing face only in a single ink color, including construction ..... per envelope ..... $_____

(i) Mailing Window Envelope (No.10):
Printing face only in a single ink color, including construction ..... per envelope ..... $_____

III. ADDITIONAL OPERATIONS:

Programming..... per hour ..... $_____

LOCATION OF POST OFFICE: All mailing will be made from the _____

Post Office located at 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 agrees, if this bid is accepted within _____ calendar days (60 calendar days unless a different period is inserted by the bidder) from the date for receipt of bids, to furnish the specified items at the price set opposite each item, delivered at the designated point(s), in exact accordance with specifications. Failure to provide a 60-day bid acceptance period may result in the expiration of the bid before award.

BIDDER'S NAME AND SIGNATURE: Unless a 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 per 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)

IR1052.204-9000 Submission of Security Forms and Related Materials (JUN 2021)

The Treasury Security Manual (TD P 15-71) sets forth investigative requirements for contractors and subcontractors who require staff-like access, wherever the location, to (1) IRS-owned or controlled facilities (unescorted); (2) IRS information systems (internal or external systems that store, collect, and/or process IRS information); and/or (3) IRS sensitive but unclassified (SBU) information.

"Staff-Like Access" is defined as authority granted to perform one or more of the following:

- Enter IRS facilities or space (owned or leased) unescorted (when properly badged);
- Possess login credentials to information systems (internal or external systems that store, collect, and/or process IRS information);
- Possess physical and/or logical access to (including the opportunity to see, read, transcribe, and/or interpret) SBU data; (See IRM 10.5.1 for examples of SBU data);
- Possess physical access to (including the opportunity to see, read, transcribe, and/or interpret) security items and products (e.g., items that must be stored in a locked container, security container, or a secure room. These items include, but are not limited to security devices/records, computer equipment-and identification media. For details see IRM 1.4.6.5.1, Minimum Protection Standards);or,
- Enter physical areas storing/processing SBU information (unescorted)

Staff-like access is granted to an individual who is not an IRS employee (and includes, but is not limited to: contractor/subcontractor personnel, whether procured by IRS or another entity, vendors, delivery persons, experts, consultants, paid/unpaid interns, other federal employee/contractor personnel, cleaning/maintenance personnel, etc.), and is approved upon required completion of a favorable suitability/fitness determination conducted by IRS Personnel Security.

For security requirements at contractor facilities using contractor-managed resources, please reference Publication 4812, Contractor Security & Privacy Controls. The contractor shall permit access to IRS SBU information or information system/assets only to individuals who have received staff-like access approval (interim or final) from IRS Personnel Security.

Contractor/subcontractor personnel requiring staff-like access to IRS equities are subject to (and must receive a favorable adjudication or affirmative results with respect to) the following eligibility/suitability pre- screening criteria, as applicable:

- IRS account history for federal tax compliance (for initial eligibility, as well as periodic checks for continued compliance while actively working on IRS

contracts);

- Selective Service registration compliance (for males born after 12/31/59); Contractors must provide proof of registration which can be obtained from the Selective Service website at www.sss.gov.;
- U.S. citizenship/lawful permanent residency compliance; If foreign-born, contractors must provide proof of U.S. citizenship or Lawful Permanent Residency status by providing their Alien Registration Number ("A" Number);
- Background investigation forms;
- Credit history;
- Federal Bureau of Investigation fingerprint results; and,
- Review of prior federal government background investigations.

In this regard, Contractor shall furnish the following electronic documents to Personnel Security (PS) at hco.ps.contractor.security.onboarding@irs.gov within 10 business days (or shorter period) of assigning (or reassigning) personnel to this contract/order/agreement and prior to the contractor (including subcontractor) personnel performing any work or being granted staff-like access to IRS SBU or IRS/contractor (including subcontractor) facilities, information systems/assets that process/store SBU information thereunder:

- IRS-provided Risk Assessment Checklist (RAC);
- Non-Disclosure Agreement (if contract terms grant SBU access); and,
- Any additional required security forms, which will be made available through PS and the COR.

Contract Duration:

a. Contractor (including subcontractor) personnel whose duration of employment is 180 calendar days or more per year must meet the eligibility/suitability requirements for staff-like access and shall undergo a background investigation based on the assigned position risk designation as a condition of work under the Government contract/order/agreement.

b. If the duration of employment is less than 180 calendar days per year and the contractor requires staff-like access, the contractor (including subcontractor) personnel must meet the eligibility requirements for staff-like access (federal tax compliance, Selective Service Registration, and US Citizenship or Lawful Permanent Residency), as well as an FBI Fingerprint result screening.

c. For contractor (including subcontractor) personnel not requiring staff-like access to IRS facilities, IT systems, or SBU data, and only require infrequent access to IRS-owned or controlled facilities and/or equipment (e.g., a time and material maintenance contract that warrants access one or two days monthly), an IRS background investigation is not needed and will not be requested if a qualified escort, defined as an IRS employee or as a contractor who has been granted staff-like access, escorts a

contractor at all times while the escorted contractor accesses IRS facilities, or vendor facilities where IRS IT systems hardware or SBU data is stored. As prescribed in IRM 10.23.2, escorting in lieu of staff-like access for IT systems and access to SBU data (escorted or unescorted) will not be allowed.

The contractor (including subcontractor) personnel will be permitted to perform under the contract/order/agreement and have staff-like access to IRS facilities, IT systems, and/or SBU data only upon notice of an interim or final staff-like approval from IRS Personnel Security, as defined in IRM 10.23.2 – *Contractor Investigations*, and is otherwise consistent with IRS security practices and related IRMs, to include, but not limited to:

- IRM 1.4.6 – Managers Security Handbook; IRM10.2.14 – Methods of Providing Protection; and IRM 10.8.1 - Policy and Guidance.

Current Investigation Reciprocity: Individuals who possess a prior favorably adjudicated Government background investigation that meets the scope and criteria required for their position may be granted interim staff-like access approval upon verification of the prior investigation, receipt of all required contractor security forms, and favorable adjudication of IRS pre-screening eligibility/suitability checks. If their current investigation meets IRS established criteria for investigative reciprocity, individuals will be granted final staff-like access, and will not be required to undergo a new investigation beyond an approved pre-screening determination.

Flow down of clauses: The contractor shall include and flow down, in its subcontracts (or arrangements or outsourced service agreements) that entails access to SBU information by a subcontractor, at any tier, the same Federal Acquisition Regulation (FAR) and local security or safeguard clauses or provisions for protecting SBU information or information systems that apply to and are incorporated in its prime contract with IRS.

(End of clause)

IR1052.204-9001 Notification of Change in Contractor Personnel Employment Status, Assignment, or Standing (JUN 2021)

The contractor, via e-mail (hco.ps.contractor.security.onboarding@irs.gov), shall notify the Contracting Officer (CO), Contracting Officer's Representative (COR), and Personnel Security within one (1) business day of the contractor (including subcontractor) becoming aware of any change in the employment status, information access requirement, assignment, or standing of a contractor (or subcontractor) personnel under this contract or order – to include, but not limited to, the following conditions:

☐ Receipt of the personnel's notice of intent to separate from employment or discontinue work under this contract/order;

☐ Knowledge of the personnel's voluntary separation from employment or performance on this contract/order (if no prior notice was given);

☐ Transfer or reassignment of the personnel and performance of duties under this contract/order, in whole or in part, to another contract/order (and if possible, identify the gaining contract/order and representative duties/responsibilities to allow for an assessment of suitability based on position sensitivity/risk level designation);

☐ Denial of or revocation of staff-like access as determined by IRS Personnel Security;

☐ Separation, furlough or release from employment;

☐ Anticipated extended absence of more than 45 days;

☐ Change of legal name;

☐ Change to employment eligibility;

☐ Change in gender or other distinction when physical attributes figure prominently in the biography of an individual;

☐ Actual or perceived conflict of interest in continued performance under this contract/order (provide explanation); or

☐ Death.

When required by the COR, the contractor may be required to provide the information required by this clause to the IRS using the Risk Assessment Checklist (RAC) or security documents as identified by Personnel Security. The notice shall include the following minimum information:

☐ Name of contractor personnel;

☐ Nature of the change in status, assignment or standing (i.e., provide a brief non- personal, broad-based explanation);

☐ Affected contract/agreement/order number(s);

☐ Actual or anticipated date of departure or separation;

☐ When applicable, the name of the IRS facility or facilities this individual routinely works from or has staff-like access to when performing work under this contract/order;

☐ When applicable, contractor (including subcontractor) using contractor (or subcontractor) owned systems for work must ensure that their systems are updated to ensure personnel no longer have continued staff-like access to IRS work, either for systems administration or processing functions; and

☐ Identification of any Government Furnished Property (GFP), Government Furnished Equipment (GFE), or Government Furnished Information (GFI) (to include Personal Identity Verification (PIV) credentials or badges – also referred to as SmartID Cards) provided to the contractor personnel and its whereabouts or status.

☐ In the event the subject contractor (including subcontractor) is working on multiple contracts, orders, or agreements, notification shall be combined, and the cognizant COR for each affected contract or order (using the Contractor Separation Checklist (Form 14604 (Rev. 8-2016)) shall be included in the joint notification along with

Personnel Security. These documents (the RAC and security forms) are also available by email request to Personnel Security.

The vendor POC and the COR must ensure all badges, Smart Cards, equipment, documents, and other government furnished property items are returned to the IRS, systems accesses are removed, and Real Estate & Facilities Management is notified of federal workspace that is vacant.

As a rule, the change in the employment status, assignment, or standing of a contractor (or subcontractor) personnel to this contract or order would not form the basis for an excusable delay for failure to perform under the terms of this contract, order or agreement.

Flow down of clauses. The contractor shall include and flow down, in its subcontracts (or arrangements or outsourced service agreements) that entails staff-like access to SBU information by a subcontractor, at any tier, the same Federal Acquisition Regulation (FAR) and local security or safeguard clauses or provisions for protecting SBU information or information systems that apply to and are incorporated in its prime contract with IRS.

(End of clause)

IR1052.204-9002 IRS Specialized Information Technology (IT) Security Training (Role-Based) Requirements (JUN 2022)

(a) Consistent with the Federal Information Security Modernization Act of 2014 (FISMA), specialized information technology (IT) security training (role-based) shall be completed prior to access to Information Systems and annually thereafter by contractor and subcontractor personnel who have an IT security role or responsibility.

(b) Identifying contractor/subcontractor with a role or responsibility for IT security is completed by the Contractor, and verified by the COR, by completing the Risk Assessment Checklist (RAC). The roles listed in the RAC conform to those roles listed in the Internal Revenue Manual 10.8.1.2 that apply to contractor personnel. This process applies to new contractors/subcontractors, replacement personnel and for existing contractors/subcontractors whose roles change during their work on a contract. This includes, but is not limited to, having an approved elevated privilege to one or more IRS systems through the Business Entitlement Access Request System (BEARS).

(c) Prior to accessing any IT system, all contractor/subcontractor personnel must successfully complete all provisions of IR1052.204-9000 Submission of Security Forms and Related Materials.

(d) In keeping with the Security Orientation outlined in IR1052.224-9001, contractors/subcontractors designated on the Risk Assessment Checklist as performing a role shall complete approved training equal to the assigned hours within 5 business days of receiving the Personnel Security's memo approving staff-like access.

(e) Annual Requirements: Thereafter, on an annual basis within a FISMA year cycle beginning July 1st of each year, contractor/subcontractor personnel performing under this contract in the role identified herein is required to complete specialized IT security, role-based training by June 1st of the following year.

(f) Training Certificate/Notice: The contractor shall use the Government system identified by Cybersecurity to annually complete specialized IT security training (role-based). The COR will track the courses, hours completed and the adhere to the established due dates for each contractor/subcontractor personnel. Alternatively, courses may be completed outside of the Government system. Any courses taken outside of the Government system must be pre-approved by IRS Cybersecurity's FISMA Training Compliance team via the COR. Adequate information such as course outline/ syllabus must be provided for evaluation. Once a course is approved, certificates of

completion provided for each contractor/subcontractor shall be provided to COR in order to receive credit toward the required hours for the contractor/subcontractor personnel. Copies of completion certificates for externally completed course must be shared with the Contracting Officer upon request.

(g) Administrative Remedies: A contractor/subcontractor who fails to complete the specialized IT security training (role-based) requirements, within the timeframe specified, may be subject to suspension, revocation or termination (temporarily or permanently) of staff-like access to IRS IT systems.

(h) Flow down of clauses. The contractor shall include and flow down, in its subcontracts (or arrangements or outsourced service agreements) that entailsstaff- like access to SBU information by a subcontractor, at any tier, the same Federal Acquisition Regulation (FAR) and local security or safeguard clauses or provisions for protecting SBU information or information systems that apply to and are incorporated in its prime contract with IRS.

(End of clause)

IR1052.209-9002 NOTICE AND CONSENT TO DISCLOSE AND USE OF TAXPAYER RETURN INFORMATION (MAY 2018)

(a) Definitions. As used in this provision—

"Authorized representative(s) of the offeror" means the person(s) identified to the Internal Revenue Service (IRS) within the consent to disclose by the offeror as authorized to represent the offeror in disclosure matters pertaining to the offer.

"Delinquent Federal tax liability" means any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability.

"Tax check" means an IRS process that accesses and uses taxpayer return information to support the Government's determination of an offeror's eligibility to receive an award, including but not limited to implementation of the statutory prohibition of making an award to corporations that have an unpaid Federal tax liability (see FAR 9.104-5(b)).

(b) Notice. Pursuant to 26 USC 6103(a) - taxpayer return information, with few exceptions, is confidential. Under the authority of 26 U.S.C. 6103(h)(1), officers and employees of the Department of the Treasury, including the IRS, may have access to taxpayer return information as necessary for purposes of tax administration. The Department of the Treasury has determined that an IRS contractor's compliance with the tax laws is a tax administration matter and that the access to and use of taxpayer return information is needed for determining an offeror's eligibility to receive an award, including but not limited to implementation of the statutory prohibition of making an award to corporations that have an unpaid Federal tax liability (see FAR9.104-5).

> (1) The performance of a tax check is one means that will be used for determining an offeror's eligibility to receive an award in response to this solicitation (see FAR 9.104). As a result, the offeror may want to take steps to confirm it does not have a delinquent Federal tax liability prior to submission of its response to this solicitation. If the offeror recently settled a delinquent Federal tax liability, the offeror may want to take steps to obtain information in order to demonstrate the offeror's responsibility to the contracting officer (see FAR 9.104-5).

(c) The offeror shall execute the consent to disclosure provided in paragraph (d) of this provision and include it with the submission of its offer. The consent to disclosure shall be signed by an authorized person as required and defined in 26 U.S.C. 6103(c) and 26 CFR301.6103(c)-1(e)(4).

(d) Consent to disclosure. I hereby consent to the disclosure of taxpayer return information (as defined in 26 U.S.C. 6103(b)(2)) as follows:

> _____ [Insert OFFEROR NAME]

The Department of the Treasury, Internal Revenue Service, may disclose the results of the tax check conducted in connection with the offeror's response to this solicitation, including taxpayer return information as necessary to resolve any matters pertaining to the results of the tax check, to the authorized representatives of on this offer:

> _____ [Insert OFFEROR NAME]

I am aware that in the absence of this authorization, the taxpayer return information of **7599 is confidential and may not be disclosed, which subsequently may remove the offer from eligibility to receive an award under this solicitation.

[insert PERSON(S) NAME AND CONTACT INFORMATION]

I consent to disclosure of taxpayer return information to the following person(s):

_____
_____

I certify that I have the authority to execute this consent on behalf of%% Offeror Name: [Insert OFFEROR NAME]

Offeror Taxpayer Identification Number: _____[Insert Offeror Taxpayer Identification Number]

Offeror Address: _____[Insert Offeror Address]

Name of Individual Executing Consent: _____[Insert Name of Individual Executing Consent]

Title of Individual Executing Consent: _____ [Insert Title of Individual Executing Consent]

Signature: _____

Date: _____

IR1052.224-9000 Safeguards Against Unauthorized Disclosure of Sensitive but Unclassified Information (NOV 2021)

1. Treasury Directive Publication 15-71 (TD P 15-71), Chapter III – Information Security, Section 24 – Sensitive But Unclassified Information defines SBU information as 'any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (USC) (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy.' SBU may be categorized in one or more of the following groups—

- Federal Tax Information (FTI), including any information on or related to a tax return
- Returns and Return Information
- Sensitive Law Enforcement Information
- Employee and Personnel Information
- Personally Identifiable Information (PII)
- Information Collected or Created from Surveys
- Other Protected Information

2. Tax return or tax return information disclosed to the contractor can be used only for a purpose and to the extent authorized herein, and willful disclosure of any such tax return or tax return information for a purpose and to the extent unauthorized for provision of appraisal services to assist with the valuation of conservation easements 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. Any such knowing or negligent unauthorized disclosure of tax return or tax return information may also result in an award of civil damages in an amount not less than $1,000 plus costs with respect to each instance of unauthorized disclosure. These penalties are prescribed by the Internal Revenue Code, Sections 7213 and 7431; see also 26 CFR § 301.6103(n)-1.

3. Contractors who perform work at contractor (including subcontractor) managed sites using contractor or subcontractor managed IT resources shall adhere to the general guidance and specific privacy and security control requirements contained in Publication 4812, Contractor Security & Privacy Controls, IRM 10.23.2 - Personnel Security, Contractor Investigations, IRM 10.5.1 Privacy Policy, and IRM 10.8.1 - Information Technology (IT) Security, Policy and Guidance. Publication 4812 and IRM 10.5.1, 10.8.1 and 10.23.2 provide comprehensive lists of all security, privacy, information protection and disclosure controls and guidance.

4. Eligibility, Fitness and Suitability. Contractor (including subcontractor) personnel hired for work within the United States or its territories and possessions and who require staff-like access, wherever the location, to IRS-owned or controlled facilities or work on contracts that involve the design, operation, repair, or maintenance of information systems, and/or require staff-like access to SBU information, must meet the eligibility requirements under IRM 10.23.2, Personnel Security, Contractor Investigations, and shall be subject to security screening and investigative processing, commensurate with the position sensitivity level, and in accordance with IRM 10.23.2, and TD P 15-71. Contractor (including subcontractor) personnel must be found both eligible and suitable, and approved for staff- like access (interim or final) by IRS Personnel Security prior to starting work on the contract/order, and before being granted access to IRS information systems or SBU information.

5. General Conditions for Allowed Disclosure. Any SBU information, in any format, made available to or created by the contractor (including subcontractor) personnelshall be treated as confidential information and shall be used only for the purposes of carrying out the requirements of this contract. Inspection by or disclosure to anyone other than duly authorized officer or personnel of the contractor (including subcontractor) shall require prior written approval of the IRS. Requests to make such inspections or disclosures shall be addressed to the CO. Access to SBU information shall be provided on a “need to know” basis. SBU information shall never be indiscriminately disseminated, and no person shall be given access to (or allowed to retain) more SBU information than is needed for performance of their duties, and for which that individual has been authorized to receive as a result of having been successfully investigated, adjudicated, trained to receive, and what is strictly necessary to accomplish the intended business purpose and mission.

6. Nondisclosure Agreement. Consistent with TD P 15-71, Chapter II, Section 2, and IRM 10.23.2.15 - Nondisclosure Agreement for Sensitive but Unclassified Information, each contractor (including subcontractor) personnel who requires staff-like access to SBU information shall complete, sign and submit to Personnel Security – through the CO (or COR, if assigned) — an approved Nondisclosure Agreement prior to being granted staff-like access to SBU information under any IRS contract or order.

7. Training. All Contractor personnel assigned to this contract with staff-like access to SBU information must complete IRS-provided privacy and security awareness training, including the Privacy, Information Protection, and Disclosure training, as outlined in IR1052.224-9001 Mandatory IRS Security Training for Information Systems, Information Protection and Facilities Physical Access. Contractor personnel required to take the Unauthorized Access to Taxpayer Data training must attest to understanding the penalties for unauthorized access, as instructed by the COR.

8. Encryption. All SBU information must be protected at rest, in transit, and in exchanges (i.e., internal and external communications). The contractor (including subcontractor) shall employ encryption methods and tools to ensure the confidentiality, integrity, and availability of SBU information.

9. Particularly relevant to this clause are the updated sections to IRM 10.8.1 and Publication 4812 regarding email and text messages, alternative work sites, and incident management:

- For email and text messaging, the contractor shall abide by IRM 10.8.1.4.17.2.2 “Electronic Mail (Email) Security”, IRM 10.5.1.6.8 “Email” plus all subsections, and IRM 10.8.2.2.1.18 “Contractor”; or Pub. 4812 section 28.3.1 “Electronic Mail (Email) Security,”. Included are requirements on encryption, subject line content, and restrictions on personal email accounts.
- For alternate work sites the contractor shall abide by IRM 10.8.1.4.11.16 “PE-17 Alternate Work Site” or Publication 4812 section 21.16 “PE-17 Alternate Work Site,”. Included are requirements for incident reporting, encryption, and secure access.

10. Incident and Situation Reporting. Contractors and subcontractors are required to report a suspected or confirmed breach in any medium or form, electronically, verbally or in hardcopy form immediately upon discovery. All incidents related to IRS processing, information or information systems shall be reported immediately upon discovery to the CO, COR, and CSIRC. Contact the CSIRC through any of the following methods:

CSIRC Contacts: Telephone: 240.613.3606 E-mail to csirc@irs.gov

In addition, if the SBU information is or involves a loss or theft of an IRS IT asset, e.g., computer, laptop, router, printer, removable media (CD/DVD, flash drive, floppy, etc.), or non-IRS IT asset (BYOD device), or a loss or theft of hardcopy records/documents containing SBU data, including PII and tax information, the contractor shall report the incident/situation to the Treasury Inspector General for Tax Administration (TIGTA) hotline at (800) 366-4484.

11. Staff-Like Access to, Processing and Storage of Sensitive but Unclassified (SBU) Information. The contractor (including subcontractor) shall not allow contractor or subcontractor personnel to access, process or store SBU on Information Technology (IT) systems or assets located outside the continental United States and its outlying territories.

Contractors (including subcontractors) utilizing their own IT systems or assets to receive or handle IRS SBU data shall not commingle IRS and non-IRS data.

12. Disposition of SBU Information. All SBU information processed during the performance of this contract, or to which the contractor (or subcontractor) was given staff-like access (as well as all related output, deliverables, or secondary or incidental by-products, information or data generated by the contractor or others directly or indirectly from the source material), regardless of form or format, shall be completely purged from all data storage components of the contractor’s or subcontractorfacilities and computer systems, and no SBU/Personally Identifiable Information (PII) information will be retained by the contractor either--

☐ When it has served its useful, contractual purpose, and is no longer needed

to meet the contractor's (including subcontractor) other, continuing contractual obligations to the IRS or

☐ When the contract expires, or is terminated by the IRS (for convenience, default, or cause).

The contractor (including subcontractor) shall completely purge from its systems and any other storage, all SBU data, including PII and tax information (originals, copies, and derivative works) within 30 days of the point at which it has served its useful contractual purpose, or the contract expires or is terminated by the IRS (unless, the CO determines, and establishes, in writing, a longer period to complete the disposition of SBU data including PII and tax information).

The contractor shall provide to the IRS a written and signed certification to the COR that all SBU materials/information (i.e., case files, receipt books, PII and material, tax information, removable media (disks, CDs, thumb drives)) collected by, or provided to, the contractor have been purged, destroyed or returned.

13. Records Management.

A. Applicability

This language applies to all Contractors whose personnel create, work with, or otherwise handle Federal records, as defined in Section B, regardless of the medium in which the record exists. Contractor/subcontractor personnel are bound by the Records Management by Federal Agencies (44 U.S.C. Chapter 31) regarding the care and retention of federal records.

B. Definitions

"Federal record" as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term Federal record:

1. includes [Agency] records;
2. does not include personal materials;
3. applies to records created, received, or maintained by Contractors pursuant to their [Agency] contract; and
4. may include deliverables and documentation associated with deliverables.

C. Requirements

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chapters. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B,

and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Contractors shall ensure that all IRS data and IRS-derived data are in commercially available or open and non-proprietary format for transition (back to IRS) in accordance with the National Archives and Records Administration (NARA) disposition guidance.

4. IRS and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of IRS or destroyed except for in accordance with the provisions of IRM 1.15.5, Relocating/Removing Records, the agency records schedules and with the written concurrence of the CO. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must immediately notify the appropriate CO. The CO must report the loss using the PII Breach Reporting Form. Privacy, Governmental Liaison and Disclosure (PGLD, Incident Management) will review the PII Breach Reporting Form and alert the Records and Information Management (RIM) Program Office that a suspected records loss has occurred. The agency must report promptly to NARA in accordance with 36 CFR 1230.

5. The Contractor shall immediately notify the appropriate CO immediately upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the [contract vehicle]. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to IRS control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand-carried, mailed, emailed, or securely electronically transmitted to the CO or

address prescribed in the [contract vehicle]. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

6. The Contractor is required to obtain the approval of the CO prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and [Agency] guidance for protecting sensitive, proprietary information, and controlled unclassified information.

7. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with IRS policy.

8. The Contractor shall not create or maintain any records containing any non-public IRS information that are not specifically tied to or authorized by the contract.

9. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974, Internal Revenue Code section 6103 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

10. IRS owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which IRS shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

11. Training. All Contractor personnel assigned to this contract who create, work with or otherwise handle records are required to take IRS-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

D. Flow down of requirements to subcontractors

1. The Contractor shall incorporate the substance of this language, its terms, and requirements including this paragraph, in all subcontracts under this [contract vehicle], and require written subcontractor acknowledgment of same.

2. Violation by a subcontractor of any provision set forth in this language will be attributed to the Contractor.

3. Other Safeguards. [Insert any additional disclosure safeguards provided by the Program Office/COR or that the CO determines are necessary and in the best interest of the Government and not addressed elsewhere in the contract. If none are entered here, there are no other safeguards applicable to this contract action.]

(End of clause)

IR1052.224-9001 Mandatory IRS Security & Privacy Training for Information Systems, Information Protection and Facilities Physical Access (NOV 2022)

The Federal Information Security Modernization Act of 2014 (FISMA) requires each federal agency to provide periodic information security and privacy awareness training to all contractors/subcontractors involved in the management, use, or operation of Federal information and information systems. In addition, contractor/subcontractor personnel are subject to the Taxpayer Browsing Protection Act of 1997, which prohibits willful unauthorized inspection of returns and return information as defined in IRC 6103(b)(2) and details that any violation of the Act could result in civil and criminal penalties under IRC sections 7213, 7213A and 7431. Contractor/subcontractor personnel are subject to the Privacy Act of 1974 (5 U.S.C. 552a; Pub. L. No. 93-579), December 1974. Contractor/subcontractor personnel are bound by the Records Management by Federal Agencies (44 U.S.C. Chapter 31) regarding the care and retention of federal records.

1. The contractor must ensure all new contractor/subcontractor personnel complete all assigned briefings which are based on the responses provided on the Risk Assessment Checklist Form 14606. These responses pertaining to access to any IRS system, including basic LAN, email and internet; access to any Sensitive but Unclassified (SBU) data; and access to any IRS facility. Since new contractor/subcontractor personnel will not have access to the IRS training system, the COR shall provide softcopy versions of each briefing.

   i. Exception: Contractor personnel (including subcontractors) performing under IRS contracts with Nonprofit Agencies Employing People Who Are Blind or Severely Disabled (as described in FAR Subpart 8.7) are exempted from the aforementioned briefing requirements, unless the contractor requests access to the training, or there is a compelling justification for requiring the training that is approved by the Contracting Officer (CO). An example of this wouldbe in an instance where visually impaired personnel is assigned to perform systems development and has potential staff-like access to IRS information.

   ii. Contractor/subcontractor personnel working with IRS information at contractor-controlled facilities with no access to the IRS network will be subject to all mandatory briefing excepting the Facilities Management Physical Security briefing as outlined in Publication 4812.

   iii. Service Personnel: Inadvertent Sensitive Information Access Training

   Contractor personnel performing: (i) janitorial and cleaning services (daylight operations), (ii) building maintenance, or (iii) other maintenance and repair and need staff-like access to IRS facilities are required to complete Inadvertent Access to Sensitive Information (SBU) Access training.

   iv. Service Personnel Security and Privacy Awareness Training: Contractor

personnel providing services in the following categories are required to complete FMSS Physical Security Training:

- Medical;
- Cafeteria;
- Landscaping;
- Janitorial and cleaning (daylight operations);
- Building maintenance; or
- Other maintenance and repair

2. In combination these mandatory briefings are known as IRS Security Awareness Training (SAT). The topics covered are: Cybersecurity Awareness, Privacy Information Protection and Disclosure, Unauthorized Access to Taxpayer Data, Records Management, Inadvertent Sensitive Information Access, Insider Threat and/or Facilities Physical Security. The completion of the assigned mandatory briefings constitutes the completion of the Security Orientation.

3. The SAT must be completed by contractor/subcontractor personnel within 5 business days of successful resolution of the suitability and eligibility for staff-like access as outlined in IR1052.204-9000 Submission of Security Forms and Related Materials and before being granted access to SBU data. The date listed on the memo provided by IRS Personnel Security shall be used as the commencement date.

i. **Note**: To be authorized, all personnel must complete required training (IRS annual and role-based privacy, information protection, and disclosure training requirements, Unauthorized Access [UNAX] awareness briefings, records management briefings, and all other specialized privacy training) and background investigations before given access to SBU data (including PII and tax information). [OMB A-130]

4. Training completion process:

The contractor must submit confirmation of completed SAT mandatory briefings for each contractor/subcontractor personnel by either:

i. Using Form 14616 signed and dated by the individual and authorized contractor management entity and returned to the COR. This option is used for new contractor/subcontractor personnel and any that do not have an IRS network account.

ii. Using the IRS training system which is available to all contractors with IRS network accounts

5. Annual Training. For contracts/orders/agreement exceeding one year in length, either on a multiyear or multiple year basis, the contractor must ensure that personnel complete assigned SAT mandatory briefings annually no later than October 31st of the current calendar year. The contractor must submit confirmation of completed annual SAT on all personnel unable to complete the briefings in the IRS training systems by submitting completed Form 14616 assigned to this contract/order/agreement, viaemail, to the COR, upon completion.

6. Contractor's failure to comply with IRS privacy and security policy (to include completion and certification of SAT requirements within the timeframe specified) may be subject to suspension, revocation or termination (temporarily or permanently) of staff-like access to IRS IT systems and facilities.

7. Flow down of clauses. The contractor shall include and flow down, in its subcontracts (or arrangements or outsourced service agreements) that entailsstaff-like access to SBU information by a subcontractor, at any tier, the same Federal Acquisition Regulation (FAR) and local privacy and security or safeguard clauses or provisions for protecting SBU information or information systems that apply to and are incorporated in its prime contract with IRS.

(End of clause)

IR1052.239-9008 Information Systems and Information Security Controls for Contracting Actions Subject to Internal Revenue Manual (IRM) 10.8.1 (JUN 2021)

In performance of this contract, the contractor agrees to comply with the following requirements and assumes responsibility for compliance by its personnel and subcontractors (and their personnel):

(a) General. The contractor shall ensure IRS information and information systems are protected at all times. The contractor shall develop, implement, and maintain effective controls and methodologies in its business processes, physical environments, and human capital or personnel practices that meet or otherwise adhere to the security and privacy controls, requirements, and objectives described in applicable security and privacy control guidelines, and their respective contracts.

(b) IRM 10.5.1 and IRM10.8.1 Applicability. This contract action is subject to Internal Revenue Manual (IRM) Part 10.8.1– Information Technology (IT) Security, Policy and Guidance, and IRM 10.5.1 – Privacy Policy. The contractor shall adhere to the general guidance and specific security and privacy control standards or requirements contained in IRM10.5.1 and 10.8.1. While the IRM 10.8.1 shall apply to the requirements to access systems, and IRM 10.5.1 shall apply to access SBU data, IRS Publication 4812, Contractor Security & Privacy Controls, may also govern as addressed in another clause. It will address the requirements related to physical and personnel security that must continue to be maintained at contractor sites.

(c) Based on the Federal Information Security Modernization Act of 2014 (FISMA), and standards and guidelines developed by the National Institute of Standards and Technology (NIST), IRM 10.8.1 provides overall IT security control guidance for the IRS, and uniform policies and guidance to be used by each office, or business, operating, and functional unit within the IRS that uses IRS information systems to accomplish the IRS mission.

(d) Contractor Security Representative. The contractor shall assign and identify, in its offer, a Contractor Security Representative (CSR) and alternate CSR to all contracts requiring staff-like access to IRS information, information technology and systems, facilities, and/or assets. The CSR is the contractor's primary point for the Government on all security-related matters and the person responsible for ensuring the security and privacy of information and information systems in accordance with the terms and conditions of the contract and all applicable security controls.

(e) Flow down of clauses. The contractor shall include and flow down, in its subcontracts (or arrangements or outsourced service agreements) that entail staff-like access to SBU information by a subcontractor or agent, at any tier, the same Federal Acquisition Regulation (FAR) and local security or safeguard clauses or provisions for protecting SBU information or information systems that apply to and are incorporated in its prime contract with IRS.

(End of clause)

IR1052.239-9009 Information Systems and Information Security Controls for Contracting Actions Subject to IRS Publication 4812 (NOV 2022)

Publication 4812 Contractor Security & Privacy is an IRS specific guide to NIST SP 800-53 Release 5 when staff- like access to IRS information or information systems under contracts for services on behalf of the IRS is outside of IRS controlled facilities or the direct control of the Service (as opposed to Internal Revenue Manual 10.8.1 - Information Technology (IT) Security, Policy and Guidance, which applies when contractors are accessing IRS information and information systems at Government controlled facilities).

The IRS Publication 4812 is a living document and updated annually to reflect changes from Executive Orders, OMB requirements, NIST updates, etc. The current version of Publication 4812 is located on the irs.gov website.

In performance of this contract, the contractor agrees to comply with the following requirements and assumes responsibility for compliance by its personnel and subcontractors (and their personnel):

1. The contractor shall ensure IRS information and information systems (those of the IRS and/or the contractor, as appropriate) are protected at all times. To do so, the contractor shall develop, implement, and maintain effective controls and methodologies in its business processes, physical environments, and human capital or personnel practices that meet or otherwise adhere to the security and privacy controls, requirements, and objectives described in applicable security and privacy control guidelines, and their respective contracts.

(a) Publication 4812 applicability. This contracting action is subject to Publication 4812 – Contractor Security & Privacy Controls. Publication 4812 is available at: Publication 4812 is available at: https://www.irs.gov/pub/irs-pdf/p4812.pdf

(b) The contractor shall adhere to the general guidance and specific security control standards or requirements contained in Publication 4812. By inclusion of this clause in the contract, the most recent version of Publication 4812 is incorporated into the contract and has the same force and effect as if included in the main body of the immediate contract.

2. Flowing down from the Federal Information Security Modernization Act of 2014 (FISMA) and standards and guidelines developed by the National Institute of Standards and Technology (NIST), Publication 4812 identifies basic Technical, Operational, and Management (TOM) security and privacy controls and standards required of under contracts for services in which contractor (or subcontractor) personnel will either—

(a) Have staff-like access to, develop, operate, or maintain IRS information or information systems on behalf of the IRS (or provide related services) outside of IRS facilities or the direct control of the Service, and/or

(b) Have staff-like access to, compile, process, or store IRS SBU information on their own information systems/Information Technology (IT) assets or that of a subcontractor or third- party Service Provider, or when using their own information systems (or that of others) and on IT, or Electronic Information and Technology (EIT) (as defined in FAR Part 2) other than that owned or controlled by the IRS.

3. Unless the manual specifies otherwise, the IRS-specific requirements in Publication 4812 meet the standard from the latest version of the NIST Special Publication (SP) 800-53 Release 5 – Federal Information Systems and Organizations. The security and privacy controls, requirements, and standards described within the Publication 4812 are to be used in lieu of the common, at-large security and privacy control standards enumerated in the latest version of NIST SP 800-53 Release 5. Publication 4812 also describes the framework and general processes for conducting contractor security reviews – performed by IT Cybersecurity—to monitor compliance and assess the effectiveness of security and privacy controls applicable to any given contracting action subject to Publication 4812.

4. Contractor Security Representative. The contractor shall assign and identify, upon award, a Contractor Security Representative (CSR) and alternate CSR to all contracts requiring staff-like access to Treasury/bureau information, information technology and systems, facilities, and/or assets. The CSR is the contractor's primary point for the Government on all security-related matters and the person responsible for ensuring the security of information and information systems in accordance with the terms and conditions of the contract and all applicable security and privacy controls.

5. Flow down of clauses. The contractor shall include and flow down, in its subcontracts (or arrangements or outsourced service agreements) that entails staff-like access to SBU information by a subcontractor, at any tier, the same Federal Acquisition Regulation (FAR) and local security, privacy or safeguard clauses or provisions for protecting SBU information or information systems that apply to and are incorporated in its prime contract with IRS. IRS Publication 4812 also applies to subcontractors.

(End of clause)

IR1052.239-9010 – Information System and Information Security Control Standards and Guidelines Applicability (NOV 2022)

As part of its information security program, IRS identifies security controls for the organization's information and information systems in the following three key standards and guiding documents:

- Internal Revenue Manual (IRM) 10.8.1 – Information Technology (IT) Security, Policy and Guidance,
- IRM 10.5.1 – Privacy Policy, and
- Publication 4812 – Contractor Security & Privacy Controls.

While IRM 10.8.1 and Publication 4812 are both based on the latest version of NIST SP 800-53, they apply to different operating environments—internal and external to the organization, respectively.

The contractor, by signing its offer, hereby asserts to the best of its knowledge and belief that the security and privacy control guideline(s) most suitable and applicable to the immediate contracting action, with due consideration to its proposed approach (and work environment) for fulfilling the Government's requirements and standards for applicability described herein, is as follows (check only one block):

☐ IRM 10.8.1 ☐ Publication 4812 ☐ Both IRM 10.8.1 and Publication 4812

Unless IRS Cybersecurity, (Contractor Security Assessment - CSA) determines, through a notification to the Contractor by the CO, that a different (or a second) security control standard or guideline is warranted, the security level selected/applied for by the contractor under IR1052.239-9010 shall stand. In the event IRS Cybersecurity (Contractor Security Assessment - CSA) determines a different (or second) security control standard or guideline is warranted, the CO shall advise the contractor, in writing, of the Government determination, and reflect the correct/appropriate security control standard or guideline in the ensuing contract.

a. If Publication 4812 is selected (alone or in combination with IRM 10.8.1) as the most suitable security control guideline, the Contractor must identify, as part of its proposal submissions (or its submissions under any modification to an existing contract incorporating this clause), the most suitable security control level within the following hierarchy of security control levels (from lowest or highest):

- Software Application Development or Maintenance (SOFT)
- Networked Information Technology Infrastructure (NET)

(Refer to Publication 4812, Appendix C for guidance in selecting the security control level most suitable and appropriate to the immediate contracting action. If additional guidance is needed in selecting the security control level, contact IRS Cybersecurity (Contractor Security Assessment - CSA).

b. The contractor, by signing its offer, hereby asserts to the best of its knowledge and belief that the security control level under Publication 4812 most suitable and applicableto the immediate contracting action, with due consideration to its proposed approach (and work environment) and standards for applicability described herein, is as follows (check onlyone):

☐ SOFT ☐ NET

c. Unless IRS Cybersecurity (Contractor Security Assessment - CSA) determines that a different (higher or lower) security control level is warranted for contracts subject to the most recent version of Publication 4812, the security level selected/applied for by the contractor will govern throughout the life of the contract. In the event the IRS Cybersecurity (Contractor Security Assessment - CSA) determines a different (higher or lower) security level is warranted, the CO will advise the contractor, in writing, of the Government determination. At the end of the contract, for all security levels, the contractor must provide a plan and document the implementation of this plan to ensure that all hard copy and electronic data is returned to the IRS, sanitized, ordestroyed.

d. Failure by the contractor to check any block will result in the use of both guidelines (for the Publication 4812 portion, use of the most stringent security control level (Software)) until and unless IRS Cybersecurity (Contractor Security Assessment - CSA), determines otherwise via notification to the Contractor by the CO.

e. Flow down of clauses. The contractor shall include and flow down, in its subcontracts (or arrangements or outsourced service agreements) that entailsstaff-like access to SBU information by a subcontractor, at any tier, the same Federal Acquisition Regulation (FAR) and local security or safeguard clauses or provisions for protecting SBU information or information systems that apply to and are incorporated in its prime contract with IRS.

(End of provision)

IRS CUSTOMER EXPERIENCE SURVEY

OMB # 1545-1432

EXCISE TAX AUDIT OR REGISTRATION REVIEW

The IRS is trying to improve its service to the public. You can help in this important mission by providing your feedback below. This voluntary survey should take less than 5 minutes to complete. Your identity will not be provided to the IRS. If you have any questions about this survey, you may call the Survey Helpline at 800-521-7177. Please use black or blue ink to complete the survey.

The following questions ask your opinion regarding how the IRS handled your most recent Excise Tax audit or Form 637 registration review. For each question, regardless of whether you agree or disagree with the final outcome, please indicate your answer by checking the box that best represents your opinion. If a question does not apply to you, please mark "Don't Know/Not Applicable."

Q1 INITIAL REGISTRATION PROCESS

Only answer Q1a-Q1c if you submitted an initial application for a 637 registration in the past year. Otherwise, skip to Q2.

How satisfied are you with the...	Very Dissatisfied	Somewhat Dissatisfied	Neither Satisfied nor Dissatisfied	Somewhat Satisfied	Very Satisfied	Don't Know/ Not Applicable
a. Ease of filing out Form 637, Excise Tax Application for Registration	☐	☐	☐	☐	☐	☐
b. Length of time it took from when you submitted your registration application to your first appointment/contact with an auditor or reviewer	☐	☐	☐	☐	☐	☐
c. Length of time it took from your first appointment/contact with an auditor or reviewer to when you received the letter of approval or denial	☐	☐	☐	☐	☐	☐

Q2 EXCISE TAX AUDIT OR REGISTRATION REVIEW PROCESS

How satisfied are you with the...	Very Dissatisfied	Somewhat Dissatisfied	Neither Satisfied nor Dissatisfied	Somewhat Satisfied	Very Satisfied	Don't Know/ Not Applicable
a. Initial information the IRS provided (e.g., letters/notices, phone calls, IRS publications) so that you knew what to expect during the audit/review	☐	☐	☐	☐	☐	☐
b. Explanation of how long the audit/review process would take from start to finish	☐	☐	☐	☐	☐	☐
c. Explanation of why more information was needed after the initial appointment/contact	☐	☐	☐	☐	☐	☐
d. Consideration given to the information you provided	☐	☐	☐	☐	☐	☐
e. Professionalism of your auditor or reviewer	☐	☐	☐	☐	☐	☐
f. Time your auditor or reviewer took to respond to your questions	☐	☐	☐	☐	☐	☐
g. IRS communication with you throughout the audit/review process	☐	☐	☐	☐	☐	☐
h. Fairness of treatment during the audit/review	☐	☐	☐	☐	☐	☐
i. Length of the audit/review process from start to finish	☐	☐	☐	☐	☐	☐
j. Explanation of the final decision for your audit/review including any changes made	☐	☐	☐	☐	☐	☐
k. Manager's effect on your audit/review, if you communicated with the manager	☐	☐	☐	☐	☐	☐

Q3 AUDIT PROCESS ONLY

Only answer Q3a-Q3c if you completed an Excise Tax audit. Otherwise, skip to Q4.

How satisfied are you with the...	Very Dissatisfied	Somewhat Dissatisfied	Neither Satisfied nor Dissatisfied	Somewhat Satisfied	Very Satisfied	Don't Know/ Not Applicable
a. Explanation of the reason(s) for the audit	☐	☐	☐	☐	☐	☐
b. Explanation of your payment options, if there was a change	☐	☐	☐	☐	☐	☐
c. Information provided to you on how to appeal the audit findings if you did not agree	☐	☐	☐	☐	☐	☐

Q4 Regardless of whether you agree or disagree with the final outcome, how would you rate your overall satisfaction with the way your Excise Tax audit or registration review was handled?

- ☐ Very Dissatisfied
- ☐ Somewhat Dissatisfied
- ☐ Neither Satisfied nor Dissatisfied
- ☐ Somewhat Satisfied
- ☐ Very Satisfied
- ☐ Don't Know/Not Applicable

Q5a Did you request any changes with regard to your registration review or audit? *[Example: requested a suspension of the audit/review]*

- ☐ Yes
- ☐ No → **SKIP TO Q6**

Q5b If a change was requested, what was the reason for your request?

Q6 Were you informed about the status of your audit/review throughout the audit/review process?

- ☐ Yes
- ☐ No

Q7 With regard to this audit/review, are you...

- ☐ The taxpayer
- ☐ A tax professional who represented the taxpayer
- ☐ Someone else who represented the taxpayer

If you are NOT the Taxpayer, skip to Q9

Q8 If you are the taxpayer, did you...

- ☐ Use a tax professional to represent you for this audit/review
- ☐ Represent yourself
- ☐ Both

Q9 Rate your level of agreement with: This interaction increased my trust in the IRS.

- ☐ Strongly Disagree
- ☐ Somewhat Disagree
- ☐ Neither Agree nor Disagree
- ☐ Somewhat Agree
- ☐ Strongly Agree

Q10 Please provide any comments or suggestions for improvement.

Occasionally, we conduct additional in-depth IRS-related research. Research participants may receive a small monetary incentive to participate depending on the research. If you are interested in participating in future research, please provide us with your telephone number and your email address (if available). This information will not be shared with the IRS and will be used only for the purpose of survey research.

Telephone number: ☐☐☐☐☐☐☐☐☐☐

Enter your 10-digit phone number
Print one digit in each square

Email address:

Enter your email address using all capital letters.

If you have been unable to resolve any specific problems with your tax matter through the normal IRS channels, or face a significant hardship due to the application of tax law, we encourage you to contact the Taxpayer Advocate Service at 1-877-777-4778 or www.taxpayeradvocate.irs.gov.

Privacy Act and Paperwork Reduction Act Notice

Our authority for requesting information with this survey is U.S.C. Section 301, and 26 U.S.C. Sections 7801, 7803, and 7805. The information you provide allows the IRS to analyze interactions between the IRS and taxpayers. This information will also help us to improve taxpayer service. Data collected will be shared with IRS staff, but your responses will be used for research and aggregate reporting purposes only and will not be used for other non-statistical or non-research purposes. The information that you provide will be protected as required by law. We estimate that it will take 5 minutes to complete this survey, including the time for reviewing instructions and completing the collection of information. Providing the information is voluntary; not providing all or part of the information requested will have no impact on you but may reduce our ability to address taxpayer concerns regarding taxpayer service. We may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB control number. The OMB number for this survey is 1545-1432. Send comments regarding this burden estimate for completing the survey or any other aspect of this collection of information, including suggestions for reducing this burden to: IRS, Special Services Section, SE:W:CAR:MP:T:M:SP, Room 6129, 1111 Constitution Avenue, NW, Washington, DC 20224.

Thank you for completing the survey.

Please return this questionnaire to Fors Marsh, PO Box 5703, Hopkins, MN 55343-5703.

12345678901234620160l 000001

Form **15039**
(November 2019)

Department of the Treasury - Internal Revenue Service

Internal Revenue Service (IRS) Customer Satisfaction Survey - Examinations

OMB Number
1545-1432

You can help the IRS improve its service to the public by answering the questions below. This voluntary survey should take less than eight minutes to complete.

Your responses will be kept anonymous to the IRS. Only aggregate information will be provided to the IRS.

The following questions ask your opinion regarding your most recent IRS examination. Regardless of whether you agree or disagree with the final outcome, please mark the appropriate circle on the scale provided.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Don't Know /Not Applicable
Q1. Regardless of the outcome, I am satisfied with the way the IRS handled my case.	1	2	3	4	5	NA
Q2. From first notice to final resolution, I am satisfied with the length of the process.	1	2	3	4	5	NA
Q3. I am satisfied with how well the IRS communicated with me (in person, in writing, or by telephone) throughout the process.	1	2	3	4	5	NA
Q4. The IRS employee clearly explained to me (in person, in writing, or by telephone) what I would need to do to prepare for the initial meeting (opening conference).	1	2	3	4	5	NA
Q5. The IRS employee clearly explained my taxpayer rights.	1	2	3	4	5	NA
Q6. The IRS employee clearly explained the examination process.	1	2	3	4	5	NA
Q7. The IRS employee was able to thoroughly answer my questions.	1	2	3	4	5	NA
Q8. The IRS employee responded to my inquiries in a timely manner.	1	2	3	4	5	NA
Q9. The IRS employee was courteous.	1	2	3	4	5	NA

Q10. After the initial request, did the IRS employee ask you to provide additional information?	1 Yes	
	2 No	Skip to 13
	3 Don't know/Not Applicable	Skip to 13

Please continue on back ▶

12345678901234620160l 000002

Form **15039**
(November 2019)

Department of the Treasury - Internal Revenue Service

Internal Revenue Service (IRS) Customer Satisfaction Survey - Examinations

OMB Number
1545-1432

You can help the IRS improve its service to the public by answering the questions below. This voluntary survey should take less than eight minutes to complete.

Your responses will be kept anonymous to the IRS. Only aggregate information will be provided to the IRS.

The following questions ask your opinion regarding your most recent IRS examination. Regardless of whether you agree or disagree with the final outcome, please mark the appropriate circle on the scale provided.

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Don't Know /Not Applicable
Q1. Regardless of the outcome, I am satisfied with the way the IRS handled my case.	1	2	3	4	5	NA
Q2. From first notice to final resolution, I am satisfied with the length of the process.	1	2	3	4	5	NA
Q3. I am satisfied with how well the IRS communicated with me (in person, in writing, or by telephone) throughout the process.	1	2	3	4	5	NA
Q4. The IRS employee clearly explained to me (in person, in writing, or by telephone) what I would need to do to prepare for the initial meeting (opening conference).	1	2	3	4	5	NA
Q5. The IRS employee clearly explained my taxpayer rights.	1	2	3	4	5	NA
Q6. The IRS employee clearly explained the examination process.	1	2	3	4	5	NA
Q7. The IRS employee was able to thoroughly answer my questions.	1	2	3	4	5	NA
Q8. The IRS employee responded to my inquiries in a timely manner.	1	2	3	4	5	NA
Q9. The IRS employee was courteous.	1	2	3	4	5	NA

Q10. After the initial request, did the IRS employee ask you to provide additional information?	1 Yes	
	2 No	Skip to 13
	3 Don't know/Not Applicable	Skip to 13

Please continue on back ▶

Form **13257-F** (Rev. September 2021) Department of Treasury - Internal Revenue Service OMB# 1545-2250

IRS WAGE & INVESTMENT CUSTOMER SATISFACTION
ACCOUNTS MANAGEMENT/ADJUSTMENTS

The IRS is trying to improve the service it provides taxpayers. You can help in this important mission by answering the questions below. This voluntary survey should take less than 7 minutes to complete. Your responses will be kept as anonymous as allowed by law to the IRS. If you have any questions about this survey, you may call the Survey Helpline at 1-888-461-8974 or email them at irssurvey@icf.com.

The following survey is concerned with any adjustments made to your originally filed tax return. These include the submission of correspondence, a second 1040, 1040X, 1040EZ, 1040A, or any adjustment to your originally filed tax return.

Privacy Act and Paperwork Reduction Act Notice

Our authority for requesting information with this survey is 5 U.S.C. Section 301, and 26 U.S.C. Sections 7801, 7803, and 7805. The information you provide allows the IRS to analyze interactions between the IRS and taxpayers. This information will also help us to improve taxpayer service.

Data collected will be shared with IRS staff, but your responses will be used for research and aggregate reporting purposes only and will not be used for other non-statistical or non-research purposes. The information that you provide will be protected as required by law. We estimate that it will take 7 minutes to complete this survey, including the time for reviewing instructions and completing the collection of information. Providing the information is voluntary; not providing all or part of the information requested will have no impact on you but may reduce our ability to address taxpayer concerns regarding taxpayer service.

We may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB control number. The OMB number for this survey is 1545-2250. Send comments regarding this burden estimate for completing the survey or any other aspect of this collection of information, including suggestions for reducing this burden to: IRS, Special Services Section, SE:W:CAR:MP:T:M:SP, Room 6129, 1111 Constitution Avenue, NW, Washington, DC 20224.

1 **Do you recall having written contact with the IRS regarding your tax return within the last 365 days?**
- (1) Yes (Reply to question 2)
- (2) No (Skip to question 3)

2 **Was the first contact made by you or by the IRS?**
- (1) By me
- (2) By the IRS

3 **Did you file an amended return to the IRS within the last year?**
- (1) Yes (Reply to question 4)
- (2) No, I did not file an amended return (Skip to question 5)

4 **Did you file the amended return because a notice or letter from the IRS instructed you to do so?**
- (1) Yes, the notice prompted me to file an amended return
- (2) No, I filed an amended return, but not because I received a notice or letter

5 **Regardless of whether you agree or disagree with the outcome,** how would you rate your overall satisfaction with the way your issue was handled?

Very Dissatisfied	Somewhat Dissatisfied	Neither Satisfied nor Dissatisfied	Somewhat Satisfied	Very Satisfied	Not Applicable
(1)	(2)	(3)	(4)	(5)	(6)

For the following questions, please focus on the outcome of the issue you recently resolved with the IRS.

6 **How satisfied were you...**

	Very Dissatisfied	Somewhat Dissatisfied	Neither Satisfied nor Dissatisfied	Somewhat Satisfied	Very Satisfied	Not Applicable
A. With the outcome of your recent issue with the IRS?	(1)	(2)	(3)	(4)	(5)	(6)
B. That your outcome was appropriate based on information you provided the IRS?	(1)	(2)	(3)	(4)	(5)	(6)

For the next set of questions, **regardless of your satisfaction with the outcome** of your issue, please focus on the **process and procedures** that the IRS used to address and resolve your issue.

7

How satisfied were you with the...	Very Dissatisfied	Somewhat Dissatisfied	Neither Satisfied nor Dissatisfied	Somewhat Satisfied	Very Satisfied	Not Applicable
A. Ease of getting more information about your issue from the IRS?	1	2	3	4	5	6
B. Ease of providing information requested by the IRS?	1	2	3	4	5	6
C. Length of time it took to resolve the issue?	1	2	3	4	5	6
D. Extent to which the IRS used accurate information about you to process your issue?	1	2	3	4	5	6

For the next set of questions, **regardless of your satisfaction with the outcome** of your issue, please focus on the **clarity and timeliness of the information** regarding your issue that was provided by the IRS.

8

How satisfied were you with the...	Very Dissatisfied	Somewhat Dissatisfied	Neither Satisfied nor Dissatisfied	Somewhat Satisfied	Very Satisfied	Not Applicable
A. Ease of understanding the initial notice and what was requested of you?	1	2	3	4	5	6
B. Completeness of instructions you received for resolving your issue?	1	2	3	4	5	6
C. Ease of understanding responses from the IRS?	1	2	3	4	5	6
D. IRS keeping you informed about the status of your case?	1	2	3	4	5	6
E. Explanation regarding the resolution of your issue?	1	2	3	4	5	6

For the next set of questions, **regardless of your satisfaction with the outcome** of your issue, please focus on the **personal treatment** you received throughout the process of resolving your issue.

9

How satisfied were you with the...	Very Dissatisfied	Somewhat Dissatisfied	Neither Satisfied nor Dissatisfied	Somewhat Satisfied	Very Satisfied	Not Applicable
A. Tone of the written IRS correspondence concerning your issue?	1	2	3	4	5	6
B. Politeness of any individuals you spoke with at the IRS concerning your issue?	1	2	3	4	5	6

10 If you were 'very dissatisfied' or 'dissatisfied' with any of the aspects in questions 5-9 above, please provide a brief explanation of why you gave this rating in the box provided.

11 **Please mark the topic that best describes your main issue.**
1. Status of refund
2. Status of payment
3. Penalty/Interest charges
4. Earned income credit
5. Exemptions/Dependents
6. Name/Address changes
7. Credits (child care, education, etc.)
8. Identity theft
9. Other changes or attachments to original return not specified in list

12 **For this recent interaction, how many days elapsed between the time you submitted your correspondence or amended return and the time you received a reply?**
1. Less than 15 days
2. 15-29 days
3. 30-44 days
4. 45-60 days
5. Over 60 days
6. Did not receive a reply

13 **What do you think is a reasonable time frame to wait for the IRS to respond to your issue?**
1. Less than 15 days
2. 15-29 days
3. 30-44 days
4. 45-60 days
5. Over 60 days

14 **Was your issue with the IRS completely resolved?**
1. Yes
2. No (Skip to question 16)
3. Not Sure (Skip to question 16)

15 **How many days did it take to resolve your issue from the time you contacted, or were contacted by, the IRS about this issue?**
1. Less than 15 days
2. 15-29 days
3. 30-44 days
4. 45-60 days
5. Over 60 days

16 **Who represented you while resolving your issue?**

	Yes	No
A. A tax professional	1	2
B. Yourself	1	2
C. An individual with tax knowledge	1	2
D. Other (Please specify) _____	1	2

17 **Did you use any of the following methods to contact the IRS about this issue?**

	Yes	No
A. Email	1	2
B. Mail	1	2
C. Toll-free line	1	2
D. In person	1	2
E. Other (Please specify) _____	1	2

18 **Have you contacted the IRS about the same issue for any prior year's tax return?**

1 Yes
2 No (Skip to question 20)

19 **How would you rate the level of service received from this contact versus previous contacts?**

1 Better
2 Worse
3 The same

20 **Regardless of the outcome of your case, how much do you agree with the following statements?**

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not Applicable
A. I received a clear description of the Adjustments process	1	2	3	4	5	M
B. My experience reflected the described Adjustments process	1	2	3	4	5	M
C. I had the opportunity to provide information important to my case	1	2	3	4	5	M
D. I was treated with respect during the Adjustments process	1	2	3	4	5	M

21 **Overall, how well did the IRS meet your expectations while handling your Adjustments case?**

1 Much Worse Than Expected
2 Worse Than Expected
3 As Expected
4 Better Than Expected
5 Much Better Than Expected

22 **If you answered "Worse than expected" or "Much worse than expected" to the above question, can you describe what caused you to feel that way?**

_____
_____
_____

Occasionally, we conduct additional in-depth IRS-related research. Research participants may receive a small monetary incentive to participate depending on the research. If you are interested in participating in future research, please provide us with your telephone number and your email address (if available). This information will not be shared with the IRS and will be used only for the purpose of survey research.

Phone Number: _____ **Email Address:** _____

23 **Use this space for comments or suggestions for improvements.**

_____
_____
_____

Thank you for completing the survey.

Please return the questionnaire to

ICF
980 Beaver Creek Drive
Martinsville, VA 24112

EXHIBIT B1

EXHIBIT B1 - Typical W&I & SB/SE Accelerated Schedule (5-3-5-10)

Qtr.	Sample Month	Contractor receives print files	Pre-note Mails	Survey 1 Mails	Postcard Mails	Survey 2 Mails
1st quarter - 2023	Oct	Wed 11/08/23	Thu 11/16/23	Tue 11/21/23	Wed 11/29/23	Wed 12/13/23
1st quarter - 2023	Nov	Fri 12/08/23	Fri 12/15/23	Wed 12/20/23	Thu 12/28/23	Fri 01/12/24
1st quarter - 2023	Dec	Mon 01/08/24	Tue 01/16/24	Fri 01/19/24	Fri 01/26/24	Fri 02/09/24
2nd quarter - 2024	Jan	Thu 02/08/24	Thu 02/15/24	Wed 02/21/24	Wed 02/28/24	Wed 03/13/24
2nd quarter - 2024	Feb	Fri 03/08/24	Fri 03/15/24	Wed 03/20/24	Wed 03/27/24	Wed 04/10/24
2nd quarter - 2024	March	Mon 04/08/24	Mon 04/15/24	Thu 04/18/24	Thu 04/25/24	Thu 05/09/24
3rd quarter 2024	April	Wed 05/08/24	Wed 05/15/24	Mon 05/20/24	Tue 05/28/24	Tue 06/11/24
3rd quarter 2024	May	Fri 06/07/24	Fri 06/14/24	Thu 06/20/24	Thu 06/27/24	Fri 07/12/24
3rd quarter 2024	June	Mon 07/08/24	Mon 07/15/24	Thu 07/18/24	Thu 07/25/24	Thu 08/08/24
4th quarter 2024	July	Thu 08/08/24	Thu 08/15/24	Tue 08/20/24	Tue 08/27/24	Wed 09/11/24
4th quarter 2024	August	Mon 09/09/24	Mon 09/16/24	Thu 09/19/24	Thu 09/26/24	Thu 10/10/24
4th quarter 2024	September	Tue 10/08/24	Wed 10/16/24	Mon 10/21/24	Mon 10/28/24	Tue 11/12/24
Forms:	14387 (W&I)	13257-F (W&I)	14054 (W&I)	13257-B (SB/SE)	13257-D (SB/SE)	13257-D (SP) (SB/SE)
	13257-K (SB/SE)	13257-K (OS) (SB/SE)	13257-L (SB/SE)	13257-L (OS) (SB/SE)	13523 (SB/SE)	13523 (OS) (SB/SE)
	13423 (SB/SE)	14384 (SB/SE)	14386 (SB/SE)			

Accelerated Mailing and Deliverable Schedule for W&I Injured Spouse Customer Satisfaction Survey OY3						
Sample Months	Quarter	GPO contractor receives print file (by 8th day of the month)	Wave 1 Mail Date (Pre-note) (by 5 BDs after GPO receives file)	Wave 2 Mail Date (1st Survey Package) (by 3 BDs after Wave 1 mailing)	Wave 3 Mail Date (postcard reminder) (by 5 BDs after Wave 2 mailing)	Wave 4 Mail Date (2nd Survey package) (by 10 BDs after Wave 3 mailing)
Jan data on Feb schedule 2024		3/8/24	3/15/24	3/20/24	3/27/24	4/10/24
Feb data on March schedule 2024		4/8/24	4/15/24	4/18/24	4/25/24	5/9/24
March data on April schedule 2024	**FY24Q2**	5/8/24	5/15/24	5/20/24	5/28/24	6/11/24
April data on May schedule 2024		6/7/24	6/14/24	6/20/24	6/27/24	7/12/24
May data on June schedule 2024		7/8/24	7/15/24	7/18/24	7/25/24	8/8/24
June data on July schedule 2024	**FY24Q3**	8/8/24	8/15/24	8/20/24	8/27/24	9/11/24
July data on August schedule 2024		9/9/24	9/16/24	9/19/24	9/26/24	10/10/24
Aug data on Sept schedule2024		10/8/24	10/16/24	10/21/24	10/28/24	11/12/24
Sept data on Oct schedule 2024	**FY24Q4**	11/8/24	11/18/24	11/21/24	11/29/23	12/13/24
Oct data on Nov schedule 2023		12/8/23	12/15/23	12/20/23	12/28/23	1/12/24
Nov data on Dec schedule 2023		1/8/24	1/16/24	1/19/24	1/27/23	2/9/24
Dec data on Jan schedule 2024	**FY24Q1**	2/8/24	2/15/24	2/21/24	2/28/24	3/13/24

EXHIBIT B3 - Typical SB/SE ACSS and CSCO Schedule (5-3-5-10)							
Qtr.	Sample Month	DRC receives print file	Pre-note Mails	Survey 1 Mails	Postcard Mails	Survey 2 Mails	
1st quarter - 2023	Oct	Wed 11/15/23	Wed 11/22/23	Tue 11/28/23	Tue 12/05/23	Tue 12/19/23	11/10 & 11/23 holidays
1st quarter - 2023	Nov	Fri 12/15/23	Fri 12/22/23	Thu 12/28/23	Fri 01/05/24	Mon 01/22/24	12/25, 1/1, & 1/15 holidays
1st quarter - 2023	Dec	Tue 01/16/24	Tue 01/23/24	Fri 01/26/24	Fri 02/02/24	Fri 02/16/24	1/15 holiday
2nd quarter - 2023	Jan	Thu 02/15/24	Fri 02/23/24	Wed 02/28/24	Wed 03/06/24	Wed 03/20/24	2/19 holiday
2nd quarter - 2023	Feb	Fri 03/15/24	Fri 03/22/24	Wed 03/27/24	Wed 04/03/24	Wed 04/17/24	
2nd quarter - 2023	March	Mon 04/15/24	Mon 04/22/24	Thu 04/25/24	Thu 05/02/24	Thu 05/16/24	
3rd quarter 2024	April	Wed 05/15/24	Wed 05/22/24	Tue 05/28/24	Tue 06/04/24	Tue 06/18/24	5/27 holiday
3rd quarter 2024	May	Fri 06/14/24	Mon 06/24/24	Thu 06/27/24	Fri 07/05/24	Fri 07/19/24	6/19 & 7/4 holidays
3rd quarter 2024	June	Mon 07/15/24	Mon 07/22/24	Thu 07/25/24	Thu 08/01/24	Thu 08/15/24	
4th quarter 2024	July	Thu 08/15/24	Thu 08/22/24	Tue 08/27/24	Wed 09/04/24	Wed 09/18/24	9/2 holiday
4th quarter 2024	August	Mon 09/16/24	Mon 09/23/24	Thu 09/26/24	Thu 10/03/24	Fri 10/18/24	10/14 holiday
4th quarter 2024	September	Tue 10/15/24	Tue 10/22/24	Fri 10/25/24	Fri 11/01/24	Mon 11/18/24	11/11 holiday
Forms:	13257-A	14755					

EXHIBIT B4 - Typical TE/GE Schedule (5-3-5-15)						
Qtr.	**Sample Month**	**MRF Sends Sample File**	**Pre-note Mails**	**Survey 1 Mails**	**Postcard Mails**	**Survey 2 Mails**
1 2012	Oct	Thu 11/15/12	Fri 11/22/13	Thu 11/28/13	Wed 12/05/12	Thu 12/27/12
1 2012	Nov	Fri 12/14/12	Sat 12/22/12	Fri 12/28/12	Sat 01/05/13	Sun 01/27/13
1 2012	Dec	Tue 01/15/13	Thu 01/24/13	Sun 01/27/13	Sun 02/03/13	Wed 02/27/13
2 2013	Jan	Thu 02/14/13	Mon 02/25/13	Thu 02/28/13	Thu 03/07/13	Thu 03/28/13
2 2013	Feb	Fri 03/15/13	Fri 03/22/13	Wed 03/27/13	Wed 04/03/13	Wed 04/24/13
2 2013	March	Mon 04/15/13	Tue 04/22/25	Thu 04/25/13	Thu 05/02/13	No wave 4
3 2013	April	Wed 05/15/13	Wed 05/22/13	Tue 05/28/13	Tue 06/04/13	Tue 06/25/13
3 2013	May	Fri 06/14/13	Fri 06/21/13	Wed 06/26/13	Wed 07/03/13	Thu 07/25/13
3 2013	June	Mon 07/15/13	Mon 07/22/13	Thu 07/25/13	Thu 08/01/13	Thu 08/22/13
4 2013	July	Thu 08/15/13	Thu 08/22/13	Tue 08/27/13	Wed 09/04/13	Wed 09/25/13
4 2013	Aug	Mon 09/16/13	Mon 09/23/13	Thu 09/26/13	Thu 10/03/13	Fri 10/10/25
4 2013	Sept	Tue 10/15/13	Tue 10/22/13	Fri 10/25/13	Fri 11/01/13	No wave 4
Form:	15039	EOE	EPE	FSLG	ITG	FEB
Form:	15084					

Form **13456**
(Novmeber 2018)

Department of the Treasury - Internal Revenue Service

IRS Publishing Postage Report

(Return this form by email using the email button above)

IRS USE ONLY					
	Agency cost code	GPO state code	GPO contractor code	Material group	
	Printing Services Specialist email address	IRS requisition number	GPO jacket number	Print order number	Program number

Instructions: Once this form is received, the contractor must: 1) Fill in the data fields below; 2) Electronically attach all postage statements to this form to create a new portable document format (PDF) file; 3) Rename the new PDF file per the contract specifications; and, 4) Use the "Submit" button at the top of this form to email the new PDF to the IRS.
DO NOT SCAN any page of Form 13456.

Name of contractor

Contact person at contractor	Contact person phone number *(include area code)*	Email address of contact person
Mailing start date *(mm/dd/yyyy)*	Mailing end date *(mm/dd/yyyy)*	☐ Mailings ☐ Wave of

ZIP Code of Post Office used for mailing	Date on Postage Statement	Pieces Mailed	Copies Mailed	Postage Amount	Postage Statement Type
(Example) 22201	1-12-2013	55,145	95,212	$12,234.56	3602-G Penalty Permit

Total number of pieces mailed	Total number of copies mailed	Total postage amount

Add Attachment | View Selected Attachment | Remove Selected Attachment

List of Attachments

Instructions for Form 13456, IRS Publishing Postage Report

Publishing Specialist Instructions: Publishing Specialists must complete the fields in the "IRS Use Only" section of the form. Once these fields are complete, use the "Lock IRS Fields" button at the top of the page to lock the fields and allow the "Email" and "Continuation Page" buttons to be visible. Then attach the Form 13456 in a separate email and send it to the contractor.

Contractor Instructions: Contractors must complete and submit via email a portable document format (PDF) file to the IRS within three (3) workdays after each turnover of the product to the USPS. Details to fill in the data fields, rename the PDF, and email the PDF are below. **Scanned pages of the Form 13456 will not be accepted.**

1) Fill in contractor and postage data fields
Form 13456 is provided as a fillable PDF file. Each field for the contractor to complete is listed below with specific instructions as needed.

- **Name of contractor**
- **Contact person at contractor's office**
- **Telephone number of contact person**
- **Email address of contact person**
- **Mailing start date:** The date the first piece is mailed
- **Mailing end date:** If not all pieces were sent on the start date, this is the date the last piece is mailed
- **Mailings: (Optional).** Check this box to note there will be multiple mailings
- **Wave: (Optional).** Check this box to note that the multiple mailings will be sent in "waves". Use the blank fields next to this check box to distinguish the number of current wave from the number of total waves.
- **Zip Code:** The ZIP code of the post office from which pieces are mailed
- **Date on Mailing Statement:** The mailing date on the postage statement
- **Pieces Mailed:** The number of envelopes, containers, or cartons, etc., that is mailed
- **Copies Mailed:** The total number of items *inside* each envelope, container, or carton, etc., that is mailed
- **Postage Amount:** The total dollar amount listed on each postage statement
- **Postage Statement Type:** Use the pull down menu to designate which type of postage statement (i.e. USPS Form 3602, 3602-R, 3605, 3600, 3607R) was used.

Form 13456 must contain only postage information for the IRS requisition number at the top of the form. Contractor **must not** combine postage associated with multiple print order/requisition numbers on a single form.

If all the lines on the front of Form 13456 are filled in, use the "**Add New Mailing Rows**" button to add another row of data fields.

2) Electronically attach postage statements to Form 13456
Use the "Add Attachment" button at the bottom of Form 13456 to attach postage statement copies. This PDF file must contain the front page of Form 13456 and all continuation sheets (if applicable); and, copies of all postage statements that are associated with the requisition number listed on Form 13456. This results in a new PDF.

3) Rename the new PDF as per the contract specifications
Prior to emailing the new PDF file, the contractor must rename the file. The PDF file must be named using nine (9) digits of the IRS Requisition Number, the first five (5) digits of the Post Office Zip Code, Mailing start date (MM/DD/YY), Mailing end date (MM/DD/YY) and .pdf (see below).

Example: For requisition number 20YY-12345, the file name will be: 20YY-12345_16625_01-02-YY_01-15-YY.pdf.

In the event the "mailing start date" and the "mailing end date" are the same, the contractor must enter the same date twice in the renamed file (see below).

Example: For requisition number 20YY-18345, the file name will be: 20YY-18345_16625_01-02-YY_01-02-YY.pdf.

4) Email the new PDF (Form 13456 with all attached postage statements)
Use the "Email to IRS . . . " button on the front of Form 13456 to email the PDF to:

- postage@publish.no.irs.gov; and, to the
- **Publishing Specialist's email address**

The PDF file should be sent in a single email when possible. The total file size of the email must be 10 MB or less. If the file size is larger than 10 MB, the contractor must create multiple PDF files, and add a suffix to the end of each file name starting with the letter "a" then "b", etc. (i.e. 20YY-18345_16625_01-02-YY_01-15-YYa.pdf).

The contractor is responsible for the accuracy of the information returned to the IRS. **Any delay or missing data could result in a delay of payment.**

EXHIBIT D1
Typical Pre-Note
(To be printed on Government Furnished Letterhead)

May 3, 2013

000001

CSCOSBXXX080799999200807
Sample A Samples
309 Sherman Ave
Palo Alto, CA 94306

Dear Sample A Samples:

I need your help with an important initiative I am undertaking to improve our service to America's taxpayers. I want to get feedback from taxpayers like you who have recently received a notice informing you of a balance due or return delinquency on your tax return.

In a few days, you will receive a questionnaire asking your opinions about the collection process with the IRS. Please direct it to the person who had the most contact with the IRS on this matter. The questionnaire should take less than 5 minutes to complete. Your answers will be combined with others to give us an evaluation of customer satisfaction with IRS service.

The primary purpose for requesting this information is to help the IRS improve its service to taxpayers. Our authority for requesting the information is 5 USC and 26 USC 7801.

Providing information is voluntary. However, if you do not answer all or part of the survey questions, the IRS may lack information it could use to improve taxpayer service. The information you provide may be disclosed to an IRS contractor when authorized by law. The contractor is required to follow confidentiality protections required by the Privacy Act and/or Internal Revenue Code section 6103.

I am committed to improving IRS service to every taxpayer. Please help me in this effort by completing and returning the questionnaire as soon as possible. If you do not receive a questionnaire, please contact the Survey Helpline at 1-866-960-7897.

Sincerely,

Denice D. Vaughan

Denice D. Vaughan
Director, Campus Compliance Services

EXHIBIT D2
Typical Pre-Note with Password
(To be printed on Government Furnished Letterhead)

August 5, 2013

45608122013Q3
John Taxpayer
12345 Survey Row
Fayetteville, NC 28301

Dear

The Internal Revenue Service (IRS), Office of Appeals needs your help to improve the services it provides to taxpayers who experience the Appeals process. The Office of Appeals is independent of any other IRS office and provides a place where disagreements about the application of tax law can be resolved on a fair and impartial basis. We are contacting taxpayers and tax professionals who have recently appealed a tax issue with the IRS Appeals office. I invite you to take part in the IRS Appeals Customer Satisfaction Survey, which asks for your opinions and feedback on how they can improve the service they provide to customers like you.

ICF International (ICF), an independent research company, is administering the survey on behalf of the Office of Appeals. The survey is available online, and I encourage you to complete the survey by typing the following link into your web browser and entering the unique password provided:

http://www.IRSAppealsSurvey.com
Password:

The primary purpose for requesting this information is to help the IRS improve its service to taxpayers. Our authority for requesting the information is 5 USC and 26 USC 7801.

Providing information is voluntary. However, if you do not answer all or part of the survey questions, the IRS may lack information it could use to improve taxpayer service. The information you provide may be disclosed to an IRS contractor when authorized by law. The contractor is required to follow confidentiality protections by the Privacy Act and/or Internal Revenue Code section 6103. The survey should take about 10 minutes to complete.

To verify the authenticity of this survey, please visit IRS.gov and enter the search term 'customer surveys.' The IRS Customer Satisfaction Survey page contains a list of valid, current, and unexpired, IRS surveys, and as of this issuance, should provide a reference to Appeals.

I am personally committed to improving service to taxpayers who use the Appeals process. Please help me in this effort by completing the survey as soon as possible. If you have any questions, problems taking this survey, or if you wish to verify the IRS sponsorship of the survey, please call the ICF Survey Help Desk at 1-800-427-4275.

Thank you in advance for your participation.

Sincerely,

Chris Wagner
Chief, Appeals
Internal Revenue Service

L1-4920

IRS WAGE AND INVESTMENT CUSTOMER EXPERIENCE SURVEY
INJURED SPOUSE

Dear

A few days ago, you received a letter from the IRS Director of Accounts Management, Wage and Investment (W&I) Division, asking for your help with an important research initiative to improve service to America's taxpayers.

We're administering a nationwide survey to gather information from taxpayers who have had contact with IRS employees and services. You were selected to receive this survey because you recently filed an Injured Spouse Allocation. We want to know your opinions about the service you received. Your responses are critical to the accuracy of our research and evaluation.

You'll find the survey attached to this letter. After you complete the survey, you can send it to us in the postage-paid reply envelope. The survey should take less than 7 minutes to complete.

Your participation is voluntary and anonymous to the IRS.

If another person had more contact with the IRS on this matter, please pass this survey along and encourage them to respond.

To verify the authenticity of this survey, you can visit **IRS.gov/CSS** and search for Injured Spouse. The page has a list of IRS surveys including (W&I), Customer Account Services, Injured Spouse.

If you have any questions about this survey, please call the Survey Helpline at 800-521-7177.

Thank you in advance for your cooperation. Your opinions will help us improve the service the IRS provides.

Sincerely,

K Wyborski

Kimberly Wyborski
Senior Director, Survey Operations Data Collection

EXHIBIT E2
Typical Explanation Letter with Password

ICF Business Operations Center

IRS Surveys
980 Beaver Creek Drive
Martinsville, VA 24112-2177

May 10, 2013
000001

WISP06081234XXX200806
Sample A Samples
309 Sherman Ave
Palo Alto, CA 94306

Dear Sample A Samples:

A few days ago, you received a letter from James Clifford, Director, Compliance, Wage and Investment Division, asking for your help with an important research project.

ICF International is administering a nationwide survey among people who have had contact with the Internal Revenue Service (IRS). We want to know your opinions regarding the audit process and the service you received. Your responses are critical to the accuracy of this research. If any other person was primarily responsible for dealing with the IRS on this matter, please give the survey to that person and encourage him or her to respond.

You may complete the survey either by mail or online. If you choose to complete it online, please enter the following internet address in your web browser: **www.IRSsurvey.com**

Once you access the website for the survey, you will be asked for a unique password. Please enter the password below:

PASSWORD: 12345678A

The password will save any answers you've entered in the event of computer disruptions. ICF will not share your password with the IRS at any time during or after this study.

ICF will hold your identity anonymous and will not provide any of your identifying information to the IRS. Your answers will be grouped with others, so that no individual reply can be traced back to a person or case number.

This brief survey should take less than 5 minutes to complete. We have included a postage-paid reply envelope for you to return your completed survey. If you have any questions or concerns, please feel free to contact ICF's Survey Helpline at 1-888-260-0052.

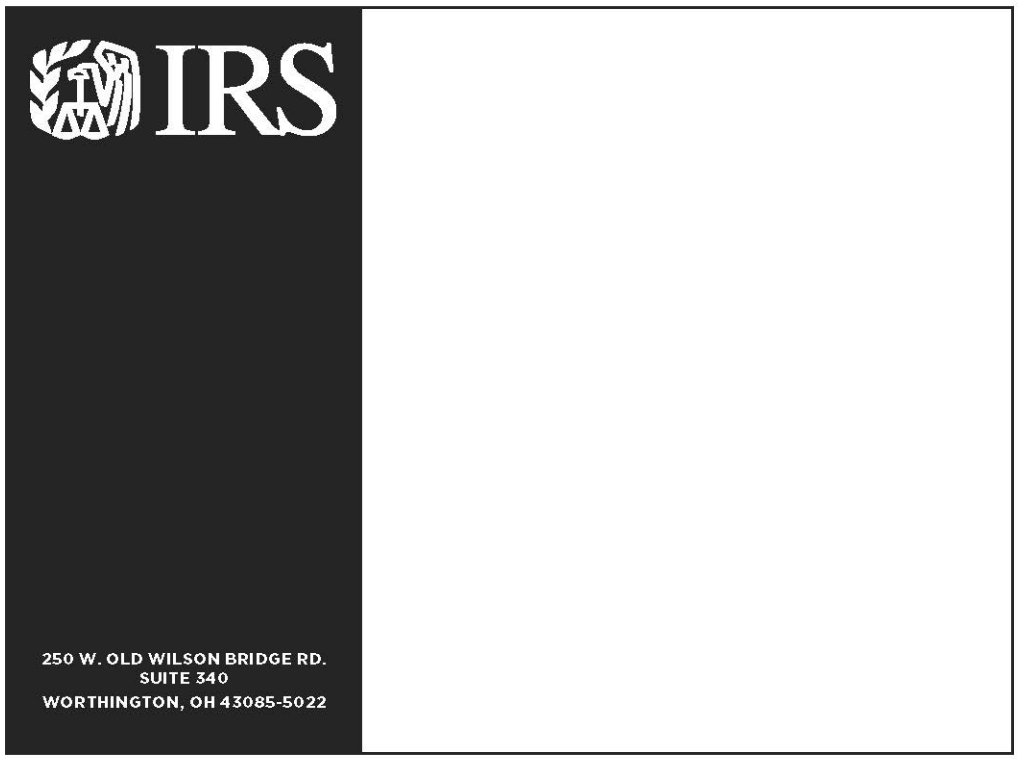
Thank you in advance for your cooperation.

Sincerely,

John Hurley
Project Director
ICF International

L2_13423

EXHIBIT F
Typical Postcard



Research
conducted by

FORS|MARSH
GROUP

Do We Have Your Input Yet?

Recently, you received a survey asking your opinions about the service you received from the IRS in a recent contact. If you have already completed and returned the survey, please accept our sincere thanks. If not, please take a few minutes to complete it and return it today. We want to be sure we have your opinions and suggestions.

If you did not receive the survey, or it got misplaced, please call us at 1-800-521-7177.

Sincerely,

Brian K. Griepentrog, Ph.D.
Director of Research
Fors Marsh Group

L3_13257-F

Form 14573 Survey Checklist of Scanned Mail Component

Survey Checklist of Scanned Mail Components

Instructions: The vendor is to inspect the mailing component below if the check box is marked. A positive match is required against the print order. After inspection, the vendor is to scan the actual mailing component with live data output from the vendor's printing equipment. Prior to emailing a PDF to the publishing specialist for approval, vendor will ensure personnally identifiable information (PII), such as taxpayer name and address, is not visible in the scan.

Product		Wave 1 Mail date	Wave 2 Mail date	Wave 3 Mail date	Wave 4 Mail date
Add Additional Waves					
Date of letter prints ☐ Needs inspection ☐ N/A		☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A
Revision Date ☐ Needs inspection ☐ N/A		☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A
MRF Envelopes ☐ Needs inspection ☐ N/A		☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A
Director's Name on Prenote ☐ Needs inspection ☐ N/A		☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A
Reference to new director on first line of Cover Letter 1 ☐ Needs inspection ☐ N/A		☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A
Matching Separate Cover Letter 1 to Survey 1 ☐ Needs inspection ☐ N/A		☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A
Reference to new director on first line of Cover Letter 2 ☐ Needs inspection ☐ N/A		☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A
Matching Separate Cover Letter 1 to Survey 2 ☐ Needs inspection ☐ N/A		☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A
Postcard ☐ Needs inspection ☐ N/A		☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A
Other ☐ Needs inspection ☐ N/A		☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A	☐ Needs inspection ☐ N/A
Inspected by					
Date inspected					
Publishing Specialist approver					
Date approved					

Exhibit I

Contractor Separation Checklist

This checklist is used to separate a Contractor from an IRS contract. The checklist will be additionally used to document the return of all security items, Government Property, and ensure all items issued to the Contractor are returned to the appropriate office(s). Please refer to Policy & Procedure Memo Number 39.1(G) IR1052-204-9006, "Notification of Change in Contractor Employee Employment Status Assignment or Standing." Please complete all entries and sign. Return the checklist to: CSM@IRS.GOV

Part I – Contractor/COR Information

1. Contractor legal name		2. Contractor SEID	3. Contractor last four digits of SSN
4a. Contract number	4b. Task Order/Document Order		5. Date contractor separated
6. Reason for notification ☐ a. Separated	☐ b. Assigned to another contract		☐ c. Becoming an IRS employee
7. COR name		8. COR SEID	9. Date notified of contractor separation

Part II - Facility Access *(ensure that all Security Items are returned prior to the contractor's departure)*

Security Items	Yes	No	N/A	Identification Number	Date Returned to PSEP	Office Location
10. Issued Smart ID Card returned						
11. Issued Legacy/PAC ID Card returned						
12. Issued Building Access/Proximity Card returned						
13. Issued parking permit returned						
14. Issued key(s) to facility exterior/interior doors returned				**For keys to desks and cabinets, initiate an OS Get Service ticket is required or call 1-866-743-5748, TTY 1-866-924-3578 for assistance.**		
15. Lock combination to facility *(exterior/ interior doors)* provided to the contractor				**Initiate an OS Get Service ticket to get combination changed.**		
16. ☐ Yes, all security items returned to the local servicing Security Services office	Returned Security items should be taken or mailed to the servicing Security Services Office. "FMSS Structure Map" Map. When mailing: Place the security items in double wrapped envelopes and send via registered mail. *(Use the local mailroom requirements for registered mail).* **Provide the mailing tracking number** _____					
17. ☐ No, all security items not returned and contractor has left without returning items ☐ Is moving to a new contract and took all security items to the new contract	If the issued Security Items listed in blocks 10-14 were not returned, contact the Situation Awareness Management Center *SAMC to report the ID access card was not retrieved from the contractor. After receiving the report number, contact the servicing Security Services Office to provide the information referencing the SAMC number. Complete the above unless it is identified the contractor took all access items to the new contract. **SAMC reference number** _____					

Part III - Systems Access *(ensure that access to IRS systems/applications and telecommunication services have been deactivated prior to the contractor's departure)*

Items	Yes	No	N/A	Date Returned
18. All assigned software applications deactivated via OL5081 *(i.e., LAN, ERAP)*				

Items	Yes	No	N/A	Date Returned
19. All phone services *(i.e., VMS)* deactivated				Initiate an OS Get Service ticket.

Part IV - Government Property ***(ensure that all government property have been returned prior to the contractor's departure)***

Items	Yes	No	N/A	Bar Code	Date Returned
20. Issued government laptop returned					
21. Issued government Blackberry returned					
22. Issued government PDA returned					
23. Issued government cell phone returned					
24. Issued government pager returned					
25. Issued government PII/SBU materials/ information *(i.e., case files, receipt books, PII data and material, removable media (disks, cds, thumb drives))* collected by, or provided to, the contractor been purged or returned					
26. ☐ Yes, all government property returned	Contact Local IT EUS staff to return equipment via this email address. OS Get Service. Inform IT equipment is no longer needed and can be picked up.				
27. ☐ No, all government property not returned ☐ Is moving to a new contract and took all assigned government equipment to the new contract	If the issued Government property listed in blocks 26 and 27 were not returned, contact the Contracting Officer and the Computer Security Incident Response Center CSIRC to report items not retrieved from the contractor, unless it is identified the contractor took equipment to their new contract. **CSIRC incident number** _____				

Retain a copy of this checklist in the applicable contract file. Notify Facilities Management with date contractor space is available via an OS Get Service ticket.

Part V - Certification

I hereby certify that I have retrieved all Security items and returned to the Servicing Physical Security Office. I certify that all Government property have been recovered and returned to the appropriate offices.

COR signature	Date

Comments

For Contractor Security Management (CSM) Use Only

All separation actions have been completed

☐ Yes ☐ No

Privacy Act Notice

The Privacy Act of 1974 requires that when we ask for information about contractors, we state our legal right to do so, why we are asking for the information and how it will be used. We must also advise what could happen if the information is not provided and whether response is voluntary, required to obtain a benefit or mandatory. Our right to ask for the information is 5 U.S.C. 301 and Executive Order 93-97. We are asking for the information to document the retrieval of IRS Security items and government assets. The information may be used by the Servicing Physical Security Office and/or TIGTA if the security items are not recovered upon separation or is reported lost/stolen so that any attempted unauthorized use of the Security items may be detected and investigated.

IRM Exhibit 10.8.2-1 (09-30-2016)
Roles That Require Specialized Training

To help ensure that the appropriate number of training hours is addressed, the list includes the minimum number of security-relevant specialized training hours required per role. Individuals who serve in multiple roles are required to complete the highest of the required hours for each of the roles in which the individual serves. For example, if an individual serves in three roles with hourly requirements of 4, 4, and 8 hours respectively, the individual will have to complete, at a minimum, 8 hours of specialized training.

i. Roles with direct impact on system security (e.g., ISSOs) require 8 hours of specialized training.
ii. Roles with ancillary impact on system security (e.g., Help Desk Personnel) require 4 hours of specialized training.

Note: The roles and specialized training hours listed come from TD-P 85-01 Appendix H.

Roles	Minimum Required Specialized Training Hours
Chief Information Officer (CIO)/Chief Technology Officer (CTO)	4
Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO)	8
Authorizing Official (AO)	4
System Owner	4
Information Owner	4
Information System Security Officer (ISSO)	8
Certification Agent	4
Information System Security Manager - Overseas the cybersecurity program of an information system(s). The ISSM often works closely with the ISSO.	8

IRM Exhibit 10.8.2-1 (09-30-2016) Roles that Require Specialized Training

Cybersecurity Policy and Guidance Personnel - Individuals responsible for developing and/ or maintaining cybersecurity policy.	8
Incident Analyst/Handler/Responder/Investigator Individuals responsible for providing security operations center services to part of all of an organization. An individual with this role may or may not be a member of an incident response team (bureau CSIRC)	8
Contracting Officer's Representative for IT Contracts - Individuals	4
Network Administrator - Individuals with the responsibility of oversight and management of a network, including implementation of security requirements.	8
System Administrator - Individuals with the responsibility of oversight and management of a system, including implementation of security requirements.	8
Database Administrator - Individuals with the responsibility of oversight and management of a database, including implementation of security requiremnts.	8
System Programmer/Developer	4
Quality Assurance Personnel - Individuals responsible for ensuring the quality of an information system(s) and/ or it's data.	4
Change Management Personnel - Individuals with change management (patching, configuration changes, functionality changes, etc.,) responsibilities.	4
Help Desk/IT Services Personnel - Individuals part of the Help Desk or IT Services staff.	4

EXHIBIT J
Website Links

Website Links:

Internal Revenue Manual (IRM) 10.8.1: https://www.irs.gov/irm/part10/irm_10-008-001r

Internal Revenue Manual (IRM) 10.23.2: https://www.irs.gov/irm/part10/irm_10-023-002

Publication 4812: https://www.irs.gov/pub/irs-pdf/p4812.pdf

Publication 4812-A: https://www.irs.gov/pub/irs-pdf/p4812a.pdf

National Institute of Standards and Technology (NIST) Special Publication 800-53:
https://csrc.nist.gov/Projects/Risk-Management/publications

Proofs, Construction Samples, and Prior-to-Production Samples Distribution

NOTE: Complete addresses will be provided after award.

One (1) address in Hampton, GA will receive the following: 11 surveys (F13257-A, F13257-B, F13257-D, F13257-D(SP), F13257-K, F13257-L, F13423, F13523, F14755, F14384, F14386).

One (1) address in Pittsburgh, PA will receive the following: one (1) survey (L4920).

One (1) address in Oakland, CA will receive the following: three (3) surveys (F13917, F13917 (SP), L4900).

One (1) address in Washington, DC will receive the following: one (1) survey (F15084).

One (1) address in Jonesboro, GA will receive the following: one (1) survey (F14387).

One (1) address in Atlanta, GA will receive the following: one (1) survey (F13257-F).

One (1) address in Conyers, GA will receive the following: one (1) survey (F14054).

One (1) address in Jacksonville, FL will receive the following: two (2) surveys (F14783, F14783 (SP).

One address in Worthington, OH will receive the following: 13 surveys (F13257-B, F13257-D, F13257-D(SP), F13257-F, F13257-K, F13257-L, F13423, F13523, F14054, F14384, F14386, F14387, F15084).

One (1) address in Redwood, City, CA will receive the following: five (5) surveys (F13257-A, F14755, F13917, F13917 (SP), L4900).

One (1) address in Rockville, MD will receive the following: one (1) survey (L4920).

Two (2) addresses in Fayetteville, GA will each receive the following: All surveys.

EXHIBIT L
Physical Security Self-Assessment

Control Number	Test Case #	Publication 4812 Requirement	Test Procedures	Risk Level	Status	Justification	Recommendation
PE-1 : Physical and Environmental Protection Policy and Procedures	1	The contractor shall develop physical and environmental protection policies and procedures. The policies and procedures shall be reviewed/updated every three (3) years or if there is a significant change to facilitate implementing physical and environmental protection controls.	Examine Standard Operating Procedures for physical and environmental protections to ensure they are site specific and address protection of IRS SBU data. Ensure procedures have been reviewed and updated at least every three (3) years or sooner if there have been changes to physical and environmental protection controls. Interview key personnel who control physical controls systems and/or who are familiar with facility changes.	High	Met		
PE-2 Physical Access Authorization	1	Designated officials or designees within the contractor's organization shall develop, review, keep current, and approve the access list and authorization credentials, i.e. identification (ID) badges.	Examine Standard Operating Procedures for physical access authorization procedures and review access list to ensure only approved individuals are on the list and have authorization credentials. Interview designated personnel to ensure procedures are being followed.	High	Met		
PE-2 Physical Access Authorization	2	ID cards issued to employees and the card key inventory must be reconciled at least annually. The access list to the information and areas handling and processing SBU information shall also be updated at least annually.	Examine annual key audit and ID audits to ensure only those who have ID cards and key access to areas handing and processing SBU are authorized and fully vetted under the contract. Document the date the last audit was conducted.	Moderate	Met		
PE-2 Physical Access Authorization	3	Any time an employee departs the organization, the access list and identification badge must be updated so that access is modified or deleted within 24-hours. All lost/stolen ID cards must be reported to management, as soon as loss is identified.	Examine Standard Operating Procedures to ensure policy is in place to address requirement to update or delete access within 24-hours of employee departure. Inspect lost/stolen ID card SOP's. Validate SOP is being followed by inspecting access control records (list, badging records, keys or card access records) changes with employee departure dates/time, or lost .	High	Met		
PE-2 Physical Access Authorization	4	Contractor company with over 25 employees shall employ a badging system.	If company has over 25 employees examine company badging system to ensure badges for employees assigned to IRS work must be readily identifiable and distinct from other employee badges.	Moderate	Met		

PE-2 Physical Access Authorization	**5**	**The contractor shall have a procedure to issue, manage, and track ID cards for visitors.**	**Examine Standard Operating Procedures to ensure visitor cards are being issued and tracked. Observe visitor check-in are to ensure SOP is being followed.**	**High**	**Met**		
PE-3 Physical Access Control	**1**	**The contractor shall control all access points to the facility. The contractor shall ensure that access is authorized and verified before granting access to areas where IRS information is processed or stored.**	**Observe entry points to areas where IRS information is processed or stored to ensure access is controlled and limited to authorized individuals.**	**High**	**Met**		
PE-3 Physical Access Control	**2**	**Whenever visitors enter the area, the contractor shall capture the following information: their name, signature, assigned work area, escort, purpose of entry, and time and date of entry.**	**Examine visitor registers to ensure all required elements are being recorded.**	**Moderate**	**Met**		
PE-3 Physical Access Control	**3**	**The entry control monitor shall verify the identity of visitors by comparing the name and signature entered in the register with the name and signature of some type of photo identification card, such as a driver's license. When leaving the area, the entry control monitor or escort shall enter the visitor's time of departure.**	**Observe to ensure entry control monitor is comparing name on the visitor register to photo identification.**	**Moderate**	**Met**		
PE-3 Physical Access Control	**4**	**Each register shall be closed out at the end of each month and reviewed by the area supervisor/manager.**	**Examine visitor register to validate register is closed out each month and is being reviewed by the area supervisor/manager.**	**Moderate**	**Met**		
PE-4 Access Control for Transmission Medium	**1**	**The contractor shall physically control and monitor access to transmission lines and closets within the contractor facilities using physical safeguards. Security safeguards to control physical access to information system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.**	**Examine transmission lines and closets throughout facility to ensure security safeguards are in place.**	**Moderate**	**Met**		
PE-4 Access Control for Transmission Medium	**2**	**When transporting IRS SBU material, the contractor shall ensure that material shall be safeguarded at all times during transport.**	**Examine Standard Operating Procedures regarding transporting IRS SBU. Interview individuals who transport IRS SBU to validate they practice safeguarding procedures as**	**High**			

			described in Standard Operating Procedures.				
PE-4 Access Control for Transmission Medium	3	All shipments of SBU information (including electronic, optical or other removable media and microfilm) shall be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged.	Examine transmittal forms for timely receipt and acknowledgment of IRS SBU data.	High	Met		
PE-4 Access Control for Transmission Medium	4	All SBU information transported through the mail or courier/messenger service shall be double-sealed; that is one (1) envelope within another envelope. In addition, the address shall be contained on both the outer and inner envelope. The inner envelope shall be marked SBU with some indication that only the designated official or delegate is authorized to open it.	Examine Standard Operating Procedures to ensure all required elements are addressed. Examine marking used for inner envelope to ensure required marking procedures are being used. Interview key personnel to evaluate procedures are being followed.	High	Met		
PE-5 Access Control for Output Devices	1	The contractor shall control physical access to the information system devices that display IRS information or where IRS information is handled or processed to prevent unauthorized individuals from observing the display output.	Examine work area where IRS SBU data is processed to ensure unauthorized individuals do not have physical access to information systems containing IRS information.	High	Met		
PE-6 Monitoring Physical Access	1	The contractor shall monitor physical access to SBU information and the information systems where IRS information is stored to detect and respond to physical security incidents. Physical security Intrusion Detection Systems (IDS) can be used in conjunction with other measures to provide forced entry protection for after-hours security. Additionally, alarms for individual and document safety (fire) and other physical hazards (water pipe breaks) are recommended.	Examine areas of facility containing IRS SBU to ensure IDS is being used to monitor, control, detect and respond to physical security incidents. Document type of IDS being used (door contacts, motion sensors, access controls systems, duress, water monitoring systems for water breaks, fire and smoke alarms). Document who monitors IDS and response time (based on documented incidents and/or alarm point testing).	Moderate	Met		

PE-6 Monitoring Physical Access	**2**	**The contractor shall monitor real-time physical intrusion alarms and surveillance equipment. (CCTV's) shall have monitoring and recording capabilities, but are not required to be monitored in real-time.**	**Examine monitoring station to ensure surveillance equipment and intrusion alarms have real-time monitoring. Examine recording equipment for CCTV's. NOTE: Recording equipment shall be stored in a limited area with restricted access so recordings can't be tampered with or erased.**	**High**	**Met**		
PE-6 Monitoring Physical Access	**3**	**Physical access logs shall be reviewed annually or upon occurrence of or potential indication of an event.**	**Examine Standard Operating Procedures to ensure policy is in place and logs are reviewed annually.**	**Moderate**	**Met**		
PE-6 Monitoring Physical Access	**4**	**Private Collection Agencies shall have CCTV's that record all sensitive areas where taxpayer data is present, including but not limited to mail processing rooms.**	**Examine work areas and monitors (evaluating displayed viewing angles) where IRS SBU data is processed (including, but not limited to mail processing areas) to ensure there is adequate CCTV coverage. Examine recording storage to ensure minimum 30 day storage capability.**	**High**	**Met**		
PE-6 Monitoring Physical Access	**5**	**Private Collection Agencies shall have separate secure room for mail processing and securing payments. Physical security assessments of the mailrooms and mail processing sites shall be conducted annually.**	**Examine mail processing rooms to ensure all physical security controls are in place and being practiced.**	**Moderate**	**Met**		
PE-8 Visitor Access Records	**1**	**The contractor shall maintain visitor access records to the facility where the information system resides. The contractor shall review the visitor access records, at least annually.**	**Examine visitor access records (not required for publicly accessible areas) to ensure they contain the required elements and that they are reviewed at least annually:** **The visitor access log shall contain the following information:** **• Name and organization of the visitor,** **• Signature of the visitor,** **• Form of identification,** **• Date of access,** **• Time of entry and departure,** **• Purpose of visit, and** **• Name and organization of person visited.**	**Moderate**	**Met**		
PE-8 Visitor Access Records	**2**	**Contractors using Cloud Service Providers shall ensure that the CSP reviews visitor access logs, at least monthly.**	**Examine visitor access logs to ensure they are reviewed at least monthly.**	**Moderate**	**N/A**		

PE-8 Visitor Access Records	**3**	**Registers or logs for areas requiring highest level security awareness (includes areas designated by the Interagency Security Committee as Facility Security Level V) should be maintained for 5 years (GRS 5.6, item 110). Registers or logs for all other facility security areas (includes areas designated by the Interagency Security Committee as Facility Security Levels I through IV) should be maintained for 2 years (GRS 5.6, item 120).**	**Examine historical logs to ensure they are maintained for the time required based on facility designation.**	**Moderate**	**Met**		
PE-9 Power Equipment and Cabling	**1**	**The contractor shall protect power equipment and power cabling for the information system from damage and destruction.**	**Examine power equipment and power cabling for information systems to ensure equipment is protected in a way that protects if from physical damage and destruction. NOTE: If above ceiling, visually inspect space above ceiling to ensure compliance.**	**Moderate**	**Met**		
PE-10 Emergency Shutoff	**1**	**Access to the shutoff switches or devices shall be unobstructed and located in such a manner so personnel have safe and easy access to them. The shutoff switches or devices are to be protected from unauthorized or inadvertent activation. The capability to shut off power to the information system or individual system components in emergency situations shall be provided.**	**Examine access and location of shutoff switches to evaluate safe and easy access.**	**Moderate**	**Met**		
PE-11 Emergency Power	**1**	**The contractor shall provide a short term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a loss of primary power.**	**Examine site for UPS dedicated to information systems used to process IRS SBU data.**	**High**	**Met**		
PE-12 Emergency Lighting	**1**	**The contractor shall employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage that covers emergency exits and evacuation routes within the facility.**	**Examine site for automatic emergency exit and evacuation route lighting that activates in the event of a power outage.**	**Moderate**	**Met**		

PE-13 Fire Protection	**1**	**The contractor shall maintain fire suppression, detection, and notification (alarms) devices for the information and/or information systems. Class A and Class C fire extinguishers shall be prominently located within any office complex containing IT assets so that an extinguisher is available within 50 feet of travel. Devices shall be supported by an independent power source and appropriate for the size of the facility being protected/safeguarded.**	**Examine site for fire suppression, detection and alarms. Examine inspection dates on fire extinguisher to ensure they've been inspected in the last 12 months. Evaluate distance of travel to ensure extinguisher is located within 50 feet of travel. Examine facility size and number of devices to ensure an adequate number of devices are provided for the size of the facility. NOTE: building engineer or property manager may also provide local fire department inspection records. Ensure hardwire devices have an independent power source.**	**Moderate**	**N/A**		
PE-13 Fire Protection	**2**	**The contractor shall employ an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.**	**Examine sites with information systems, where facilities are not staff on a continuous basis to ensure the automatic fire suppression systems. Ensure system has been evaluated or inspected annually for functionality.**	**Moderate**	**N/A**		
PE-13 Fire Protection	**3**	**When the facility is used to store large volumes of SBU information in warehouse and/or storage facilities, the contractor shall ensure that sprinkler systems and/or water suppression equipment shall be in place to minimize damage to critical historical files.**	**Examine site to ensure sprinkler systems and/or water suppression equipment in in place. Ensure system has been evaluated or inspected annually for functionality. The contractor shall install separately contained/valve wet pipe, water sprinkler system (pipe scheduled or hydraulically designed type) inside the entire firewall, encapsulated computer room and tape library areas with automatic power cut--off capability. (National Fire Protection Association (NFPA) Standard No. 13 provides details on installation of acceptable sprinkler systems).**	**High**	**N/A**		
PE-14 Temperature and Humidity Controls	**1**	**The contractor shall maintain and monitor temperature and humidity levels within the facility where the information system resides. The monitoring of the temperature and humidity levels is to be continuously monitored.**	**Examine to determine if site maintains and monitors temperature and humidity levels where information systems are stored. Ensure system has been evaluated or inspected annually for functionality.**	**Moderate**	**N/A**		

PE-15 Water Damage Protection	**1**	**The contractor shall protect the information systems from damage resulting from water leakage by ensuring that master shutoff valves are accessible, working properly and known to key personnel.**	**Examine site for accessibility of master shut off valves. Ensure system has been evaluated or inspected annually for functionality. Interview key personnel to determine awareness of shut off procedures and valve locations.**	**Moderate**	**N/A**		
PE-16 Delivery and Removal	**1**	**For all IT information systems that house SBU information, the contractor shall authorize and control information system-related items entering and exiting the facility, and maintain appropriate records of those items. The authorization process shall define individuals who are authorized to remove IT related equipment and/or other records.**	**Examine procedures for delivery and removal of IT information systems that house IRS SBU information to ensure only authorized personnel control such assets. Examine records tracking movement or removal of these items. Interview individuals who are authorized to remove IT related equipment of IRS SBU data to evaluate if procedures are being followed.**	**Moderate**	**N/A**		
PE-17 Alternate Work Site	**1**	**The contractor shall develop procedures required to safeguard IRS SBU for work performed at alternate work sites such as an employees' home office. A contractor management approval process shall be in place to ensure that employees working at home are aware of their responsibilities and have the ability to protect IRS SBU. (NOTE : Federal Tax Information cannot be processed or stored at employee's home or elsewhere except as otherwise approved by IRS)**	**Examine procedures addressing safeguards for IRS SBU data at alternate work sites. Examine alternate worksite to evaluate safeguards are in place.**	**Moderate**	**Met**		
PE-17 Alternate Work Site	**2**	**The employees' home office environment shall have the following features/capabilities;• a telephone• a work space suitable to perform work• all SBU in the possession of the employee, must be kept in a locking file cabinet or drawer• secure remote network access via a VPN• a work environment that is free from interruptions and provides reasonable security and protections.**	**Examine procedures addressing safeguards for IRS SBU data at alternate work sites. Examine alternate worksite (home office environment) to evaluate required features are in place.**	**Moderate**	**Met**		

PE-17 Alternate Work Site	**3**	**Digital assistants and other devices that can record or transmit sensitive audio or visual information must not be allowed to compromise privacy in the work or telework environment.**	**Examine work sites and alternate worksites to ensure such devices are not in the work or telework environment.**	**Moderate**	**Met**		

Control Number	Test Case	Publication 4812 Requirement	Test Procedures	Status	Justification
AC-2 Account Management	1	Any time there is more than one (1) contractor using an IT asset, such as a server, network, or information system, the contractor shall configure the asset so that there is one (1) unique account created and used for each employee who shall perform IRS work on that asset.	Examine the user list of the information system and ensure that each account is tied to an individual and that there are no shared accounts.		
AC-2 Account Management	2	An account manager shall be assigned.	Examine evidence which shows to whom roles and responsibilities are assigned to ensure that the account manager role exists.		
AC-2 Account Management	6	Call recording systems shall restrict access to only staff initiating or receiving calls. Call recordings shall not be available for those not participating in the conversation except staff members performing a management designated quality assurance function.	Examine user access restrictions to ensure that only authorized staff are permitted access to the recorded transmissions		
AC-5 Separation of Duties	1	The contractor shall establish appropriate divisions of responsibilities and separations of duties as needed to eliminate conflicts of interest.	Examine Active Directory, or equivalent system tool, to determine what groups are established to show Separation of Duties is in place.		
AC-6 Least Privilege	4	Ability to install software, including adding, removing, or modifying software, unless this is part of the job responsibilities, is restricted.	Examine the IT asset to determine if the user has admin rights. Examine the roles and responsibilities document and ensure that the user is listed to have admin rights if they have it on the workstation or domain.		
AC-6 Least Privilege	5	File Transfer Protocol (FTP) or Telnet, (while FTP is a telecommunication issue, this shall be restricted in terms of least privilege as well).	Examine the workstation to determine if the user has access to FTP either through the command prompt or installed application. Check the SCAP tool report and/or the roles and responsibilities document to ensure the user is allowed those rights if they have it.		
AC-6 Least Privilege	6	Accounts with administrative privileges (including local administrator rights) shall be prohibited from web browsing, Internet connections and accessing email. This can be implemented by establishing separate accounts for privileged users. One account with admin rights for privileged duties and a standard user account without admin rights for routine business functions	Examine the user permissions for those contractor employees working on the IRS contract work to determine if local admin rights are restricted to only those authorized in the roles and responsibilities document. Verify the SA has a user account and a privileged account.		

AC-6 Least Privilege	**7**	**Backup rights to either the information system and/or server shall be restricted.**	**Examine the user access permissions for those contractor employees working on the IRS contract work to determine if the system is configured to restrict the backup rights.**		
AC-6 Least Privilege	**8**	**Elevated access rights to the database software shall be restricted.**	**Note: this control applies to contractor sites which use a database to perform IRS contract work and is N/A for all other contractor sites. For contractor sites using a database, examine the user list of the database to determine who has administrative capabilities and compare that to the roles and responsibilities document.**		
AC-6 Least Privilege	**9**	**Access to saving files to either an electronic, optical, or other removable media including floppy devices or Universal Serial Bus (USB) devices shall be restricted.**	**Determine if USB ports are restricted by examining the workstations and/or the BIOS to determine if the workstation USB and other external drives are disabled.**		
AC-6 Least Privilege	**10**	**All returns and return information and other SBU information shall be physically or logically partitioned within the information system and/or the IT environment of the contractor site, as appropriate, to ensure this sensitive information is not commingled with the information of any other party or entity, and is accessible only to authorized personnel. Partitioning can be accomplished with the use of routers & firewalls, and partitioned directories, controlled by user permissions.**	**Examine the information system where IRS information is stored/processed and determine if there are physical or logical access controls in place.**		
AC-17 Remote Access	**2**	**Anytime a contractor allows an employee or IT support employees to remotely access the contractor's IT environment that houses and/or processes IRS SBU data, the connection must be secured using a Virtual Private Network (VPN) using two-factor authentication and FIPS 140-2 or later validated encryption.**	**Examine the Access Control Policy and verify that two-factor authentication is required to successfully gain remote access into the information system. The use of two-factor authentication requires the use of: 1) something they know, such as a password and 2) something they possess, such as a token card, to access the information system. 3) what you are**		
AC-19 Access Control for Mobile Devices	**2**	**All mobile computing devices shall require and have full disk encryption. This includes, but is not limited to, IT resources, including computers, servers, laptop computers, removable Compact Disk (CD) and Digital Video Device (DVD) media, thumb drives, or any media that can be used to house IRS data that can be easily transported by an individual.**	**Examine the mobile device to determine if a FIPS 140-2 approved full disk encryption product is in use on the device.**		
AU-2 Auditable Events	**2**	**Call recording application systems must have the ability to capture and retain call recording meta-data. Meta-data associated with**	**Examine the Call Recoding system files to determine if meta-data is being captured and stored.**		

		the voice recording must include the following; • The staff member initiating or receiving the call • The data, time and duration of the conversation • A means to track the identity of the customer			
AU-3 Content of Audit Records	1	At a minimum, information systems shall generate audit records containing information that establishes: • What type of event occurred. • When the event occurred. • Where the event occurred. • The source of the event. • The outcome of the event. • The identity of any individuals or subjects associated with the event.	Examine audit records to determine if they contain sufficient information to, at a minimum, establish: what type of event occurred, when (date and time) the event occurred, where the event occurred, - the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.		
AU-5 Response to Audit Processing Failures	1	In the event that the audit records become full and/or auditing stops recording, the information system shall be configured so that an alert is generated, and appropriate management is notified to take action to ensure audit records are retained and the information system is returned to normal operations.	Examine evidence such as information system alerts; information system audit records; information system configuration settings and/or associated documentation to determine if the information system alerts contractor-defined personnel or roles in the event of an audit processing failure.		
AU-6 Audit Review, Analysis, and Reporting	1	Automated reports shall be generated, and management or designated personnel shall review reports to identify unusual activity and take action, as necessary. The contractor shall document the timeframe for when they shall be conducting reviews.	Examine evidence such as the audit plan; records of actions taken in response to reviews/analyses of audit records; other relevant documents to determine if the contractor designates the personnel or roles to review the audit logs to identify unusual activity and take action, as necessary.		
AU-6 Audit Review, Analysis, and Reporting	2	A Call recording application system must have the ability to search the meta-data for the purposes of play-back and quality assurance.	Examine technical documents to ensure that call recording meta-data is available for analysis		
AU-7 Audit Reduction & Report Generation	1	The information system shall provide an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents.	Examine the audit report configuration settings to determine if the information system provides an audit reduction and report generation capability that supports: on-demand audit review; -analysis; -reporting requirements; -after-the-fact investigations of security incidents; and does not alter the original content or time ordering of audit records.		
AU-8 Time Stamps	1	All audit records will contain a timestamp.	Examine evidence such as information system audit records; information system configuration settings; other relevant documents to determine if the contractor provides time stamps for use in audit record generation.		

AU-9 Protection of Audit Information	**1**	**Audit logs shall be protected by strong access controls to help prevent unauthorized access to ensure events are not modified or deleted. To ensure separation of duties, where possible, management of the audit logs should be an individual other than system administrator.**	**Examine information system password configuration settings; system-generated list of privileged users with access to management of audit functionality; access authorizations; access control list; information system audit records; or other relevant documents to determine if the contractor authorizes access to management of audit functionality to only the organization-defined subset of privileged users.**		
CA-5 Plan of Action & Milestones	**1**	**For any security reports issued to the contractor, including internal independent reviews, the contractor is responsible for developing a POA&M that identifies corrective actions and/or mitigating controls for any identified vulnerabilities.**	**Examine evidence such as a POA&M or other flaw tracking document.**		
CA-5 Plan of Action & Milestones	**2**	**See RA-5 (Vulnerability Scanning) for information on closure timelines for Critical and High vulnerability findings. POA&Ms shall be provided to the COR or delegate at a minimum quarterly, demonstrating progress made toward weakness remediation.**	**Examine evidence that the contractor has provided quarterly POAM updates to the COR**		
CA-6 Security Authorization	**1**	**The senior official ensures the information systems security authorization is reviewed and updated every 3 years or when a significant impact to the information system occurs.**	**Examine evidence to identify the senior official who authorizes the system authorization, i.e. is authorized to shut down the system in the event of a malicious attack. Examine evidence to show the system is authorized by a senior official.**		
CA-7 Continuous Monitoring	**1**	**The contractor shall implement a continuous monitoring strategy that includes ongoing monitoring of the security controls (e.g. monthly policy checking and vulnerability scans), in accordance with the defined configurations to identify any controls that may not be compliant.**	**Examine evidence such as a security assessment and a scanning tool report to show a continuous monitoring strategy is in place.**		
CM-6 Configuration Settings	**1**	**The contractor shall establish and document configuration settings for information technology products employed within the information system using security configuration tools. At a minimum, the assessment shall include one (1) of the following for each IT asset category in Publication 4812, Section 15.6, Table 5.**	**Examine a SCAP tool report which shows the high risk or critical vulnerabilities to determine if the contractor meets the objective of this control.**		

CM-6 Configuration Settings	2	Contractors using Cloud Service Providers shall ensure that they or the CSP verify that the configuration settings are established and documented for information technology products employed within the information system using United States Government Configuration Baseline (USGCB). If USGCB is not available, the service provider shall use the Center for Internet Security (CIS) guidelines (Level 1) to establish configuration settings.	Examine the configuration baselines for CSP devices for adherence to the required standards		
CM-7 Least Functionality	1	The contractor shall review the information system at a minimum annually to identify and eliminate unnecessary functions, ports, protocols, and/or services. The contractor shall ensure compliance with all defined requirements related to functions, ports, protocols, and services.	Examine a SCAP tool report which shows the status of functions, ports, protocols, and/or services.		
CM-11 User Installed Software	1	The contractor shall establish and enforce a policy governing the installation of software by users. Compliance with the policy shall be monitored, at least annually.	Examine the policy and procedures which explain the software installation approval path.		
CP-2 Contingency Plan	1	All contractors shall develop Contingency Plans (CP) to address IT and Physical Security planning. These shall identify key business functions provided to the IRS, alternate work sites, alternate resources, contact information, and identify the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO).	Examine the Contingency Plan to determine if it meets the requirements outlined in Publication 4812.		
CP-2 Contingency Plan	2	Contractors using Cloud Service Providers shall ensure that the CSP plans for the resumption of essential missions and business functions within twenty-four (24) hours	Examine the Cloud Service Provider's Service Level Agreement to ensure that the 24 hour RTO is stated.		
CP-6 Alternate Storage Site	2	All backup information/media/data containing SBU information shall be encrypted.	Examine evidence such as the backup tool configuration settings and/or report, to verify the backup encryption is in place and is FIPS compliant.		
CP-9 Information System Backup	1	For contractors with information systems, in order to achieve the Recovery Point Objective (RPO) and the Recovery Time Objective (RTO) of the business customer, the contractor shall back up data contained in the information systems to enable contractors to provide continuous support to IRS. The contractor shall backup information system documentation including security-related	Examine evidence detailing the backup procedures to determine if both the data and system files are backed up.		

		documentation. Backups include user-level information, system-level information, and SBU information.			
CP-9 Information System Backup	2	Contractors using Cloud Service Providers shall ensure that they or the CSP conduct backups for information contained in the information system at the following frequency: a) User-level: daily incremental; weekly full b) System-level: daily incremental; weekly full c) Information system configuration; daily incremental; weekly full	Examine the Cloud Service Providers' Service level Agreement or contractor managed backup schedules		
IA-7 Cryptographic Module Authentication	1	When contractors are employing cryptographic modules for authentication, the encryption modules shall be compliant with NIST guidance (i.e., FIPS 140-2 or later). Current FIPS 140-2 validation lists can be found at http://csrc.nist.gov/groups/STM/cmvp/validation.html.	Examine system design documentation and configuration settings to determine if the information system uses mechanisms for authentication to a cryptographic module that are compliant with NIST guidance (i.e., FIPS 140-2 or later).		
IA-7 Cryptographic Module Authentication	2	When contractors are employing cryptographic modules for Kerberos authentication, AES128_HMAC_SHA1 and AES256_HMAC_SHA1 are the only allowable encryption types.	Examine system design documentation and configuration settings to determine when contractors are employing cryptographic modules for Kerberos authentication, that the encryption type used is AES128_HMAC_SHA1 or AES256_HMAC_SHA1.		
IR-1 Incident Response Policy & Procedures	1	The contractor shall develop and document incident response policies and procedures, as these relate to IRS work.	Examine the incident response policy and procedures to determine if the contractor develops and formally documents the incident response policy and procedures that relates to the IRS work.		
IR-6 Incident Reporting	1	All incidents related to IRS processing, information or information systems shall be reported within one (1) hour to the CO, COR, and SAMC.	Examine security incident logs and/or other relevant documentation to determine if the contractor reports security incident information within one hour to the CO, COR, and IRS Situational Awareness Management Center via telephone at (866) 216-4809.		

IR-8 Incident Response Plan	**1**	**The contractor shall develop and annually review an incident response plan that provides the high-level approach to handle incidents. The plan shall provide the organization with a roadmap for implementing its incident response capability.**	**Examine evidence such as security incident logs, Incident Handling/Reporting Procedures, Incident Handling/Report reports, Incident Handling/Report resolutions/lesson learned, Incident Handling/Reporting Tracking Tools, and/or other relevant documentation to determine if the contractor develops and annually updates an incident response plan that provides the organization with a roadmap for implementing its incident response capability.**		
MA-2 Controlled Maintenance	**2**	**When off-site maintenance or repairs are required, the Contractor Security Representative (CSR) will explicitly approve, with an approval letter or form, the removal of the information system or system component from the contractor's facilities.**	**Examine maintenance records; change control records; or other relevant documents to determine if the Contractor Security Representative (CSR) will explicitly approve the removal (with an approval letter or form) of the information system components from contractor facilities for off-site maintenance or repairs.**		
MA-3 Maintenance Tools	**1**	**Maintenance equipment/tools with storage capabilities shall be properly sanitized prior to removal from the contractor site.**	**Examine maintenance plan; information system maintenance tools and associated documentation; maintenance records; other relevant documents to determine if the contractor prevents the unauthorized removal of maintenance equipment containing organizational information by sanitizing or destroying the equipment.**		
MA-4 Non-Local Maintenance	**1**	**When non-local maintenance is performed, the following shall be accomplished: the IT support shall use strong identification and authentication techniques, such as two-factor authentication or PKI. All network communications shall be terminated when work is completed.**	**Examine information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents to determine if the contractor employs strong authenticators (such as two-factor authentication or PKI) in the establishment of nonlocal maintenance and diagnostic sessions. Verify a process is in place to terminate all network communications when work is completed.**		
MA-5 Maintenance Personnel	**1**	**The contractor shall designate key personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.**	**Examine service provider contracts; service-level agreements; list of authorized personnel; maintenance records; access control records; other relevant documents to determine if the contractor designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.**		

MP-2 Media Access	**1**	**Determine if the contractor ensures that media access is restricted to prevent electronic media from being lost, stolen, or disclosed.**	**Examine procedures addressing media access restrictions; access control procedures; physical and environmental protection procedures; media storage facilities; access control records; other relevant records to determine if the organization restricts access to organization-defined types electronic media to organization-defined personnel or roles.**		
MP-6 Media Sanitization	**1**	**A log shall be maintained to provide a record of media destroyed. The log shall include: • the date of destruction; • content of media; • identifying serial number; • (type of media (CD, cartridge, etc.); • media destruction performed; • personnel performing the destruction; • and witnesses to the destruction.**	**Examine media sanitization records; other records to determine if the contractor provide a record of media destroyed. Verify the log includes: the date of destruction; content of media; identifying serial number; (type of media (CD, cartridge, etc.); media destruction performed; personnel performing the destruction; and witnesses to the destruction.**		
MP-6 Media Sanitization	**2**	**The shall have possess tools and methods to conduct sanitization of digital media that can be used in Clear and Purge operations as described in Section 20 Media Sanitization.**	**Examine that tools and/or contract support is available to provide for degaussing or other data destruction methods, sufficient to meet IRS requirements of over writing and sanitizing the data. Note: Deleting the data is not sufficient.**		
PL-2 System Security Plan	**1**	**The contractor shall develop and maintain a security plan to identify key information about the contractor site and about the security controls that shall be used to ensure that IRS information is adequately safeguarded.**	**Examine the System Security Plan (SSP) to determine if all necessary security controls are addressed as required in Publication 4812.**		
PL-8 Information Security Architecture	**1**	**The contractor shall develop and maintain an Information Security Architecture document that: describes the overall security architecture of the organization.**	**Examine evidence such as the SSP, company's infrastructure diagram or similar evidence to verify the contractor developed and maintains an Information Security Architecture document that describes the overall security architecture of the organization.**		
PS-3 Personnel Screening	**1**	**Personnel screening shall take place for all contractor personnel who work on IRS contracts. This includes employees who perform data entry, develop or write programs, perform assessments for tax purposes, perform security or telecommunications administration to the information system, or have staff-like access to data or information systems. This also includes subcontractors who support the primary contractor efforts.**	**Obtain from the COR the list of contractors having interim or staff-like access and compare that list against the contractor's domain access list to identify any contractors who have access to IRS SBU that have not been cleared.**		

PS-7 Third-Party Personnel Security	**1**	**The contractor shall establish personnel security requirements, including security roles and responsibilities for third-party providers. All subcontractors providing IT support shall meet the personnel security requirements of the primary contractor, as they have staff-like access to the data.**	**Obtain from the COR the list of contractors having interim or staff-like access and compare that list against the contractor's domain access list to identify any sub-contractors who have access to IRS SBU that have not been cleared.**		
RA-3 Risk Assessment	**1**	**For all information systems environments, a risk assessment shall be conducted by the contractor to assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency regarding the use of SBU information.**	**Examine evidence to verify a Risk Assessment has been completed and the results documented in a official report.**		
RA-5 Vulnerability Scanning	**1**	**Vulnerability scanning is a test that inspects workstations, servers, network or mobile computing devices for weaknesses or flaws. The test relies on vulnerability scanning software that shall be configured to inspect devices for missing updates, patches and common configuration problems. The software shall be configured to receive updates and have the capability to perform authenticated scanning.**	**Examine the contractor' has scanning tools in place to ensure that no vulnerabilities are introduced into the environment. At a minimum, virus detection is required to ensure malicious software is not introduced into the environment.**		
RA-5 Vulnerability Scanning	**2**	**All workstations, servers, network or mobile computing devices shall undergo monthly vulnerability scanning.**	**Examine the last scan results and note if the contractor is addressing identified risks within their internal IT environment. Verify the scans are being conducted at least monthly.**		
RA-5 Vulnerability Scanning	**3**	**When providing programming services or hosting applications or services, enhanced vulnerability scanning software shall also be used. Enhanced vulnerability scanning software is capable of inspecting source code for common security flaws and performing dynamic build testing that inspects the application for security flaws at run time.**	**If there is a public facing website, the contractor is responsible for running a vulnerability scan. Examine the last scan to ensure that the contractor is mitigating risks identified within the scans. Notes: the scan should check for SQL Injection, Cross Site Scripting.**		
RA-5 Vulnerability Scanning	**4**	**Vulnerabilities identified on the scan reports must be remediated within the following time frames; • Critical-risk vulnerabilities shall be mitigated within thirty (30) days from date of discovery; and • High-risk vulnerabilities shall be mitigated within sixty (60) days from date of discovery.**	**Examine the last 3 monthly scans to determine that critical and high vulnerabilities have bee remediated within the time frames defined in Publication 4812**		

RA-5 Vulnerability Scanning	**5**		**Examine the Cloud Service Providers' Service level Agreement or that the contractor conducts scans are conducted monthly**		
SC-7 Boundary Protection	**1**	**Any contractor who manages information system environments shall ensure that all internal and external information system boundaries are controlled using boundary protection mechanisms, e.g. routers and switches.**	**Examine the information system to determine if the information system implements sub networks for publicly accessible system components that are physically and/or logically separated from internal organizational networks. Note: This objective is verifying that DMZ or the externally facing portion of the network in quarantined.**		
SC-7 Boundary Protection	**2**	**The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).**	**Examine boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; records of traffic flow procedures exceptions; information system audit records; other relevant documents to determine if the contractor implements a managed interface for each external telecommunication service.**		
SC-8 Transmission Confidentiality and Integrity	**1**	**The information system protects the confidentiality and integrity of transmitted information. Encryption shall be compliant with FIPS 140-2 or later protection requirements.**	**Examine information system design documentation, information system configuration settings to determine if the contractor employs cryptographic mechanisms. Encryption shall be compliant with FIPS 140-2 or later protection requirements. A list of NIST validated modules is available at the following link: http://csrc.nist.gov/groups/STM/cmvp/validation.html.**		
SC-12 Cryptographic Key Establishment & Management	**1**	**The contractor shall establish and manage cryptographic keys for required cryptography employed within the information system. When public key certificates are used, the contractor shall manage key policies and/or certificates**	**Examine information system design documentation; information system configuration settings; other relevant documents to determine if the organization establishes and manages cryptographic keys for required cryptography employed within the information system.**		

SC-13 Cryptographic Protection	**1**	**When cryptography (encryption) is employed within the information system, the information system shall perform all cryptographic operations using FIPS 140-2 or later validated cryptographic modules with approved modes of operation. A list of NIST validated modules is available at the following link: http://csrc.nist.gov/groups/STM/cmvp/validation.html.**	**Examine system configuration settings, configuration documents, and/or encryption configuration settings to determine if the type of cryptography being used in the information system employs a FIPS-approved algorithm.**		
SC-23 Session Authenticity	**1**	**The information system shall provide mechanisms to protect the authenticity of communications sessions that shall validate the source and destination of communication sessions. This applies to contractors, who are developing or providing web-based applications.**	**Examine the information system to determine if the system protects the authenticity of communications sessions. Is it secured using SSL or HTTPS? NOTE: Mechanisms used to protect the authenticity of communications sessions include but are not limited to the following: • Security services based on IPsec • VPNs • TLS • DNS • SSH• SSL• Digital signatures• Digital certificates • Digital time stamping• Approved encryption requirements and technology: FIPS 140 - 2, Use of AES 128 bit or higher.**		
SC-28 Protection of Information at Rest	**1**	**All portable media shall be encrypted, including laptops, etc.**	**Examine the information system configuration settings to determine if SAN (storage area network), USB drives, backup tapes, removable hard drives, laptops, etc. containing IT System User Information, IT System-related information, PII, or FTI information should be protected with FIPS 140-2 validated or NSA approved cryptography.**		
SI-2 Flaw Remediation	**1**	**Contractors shall identify, report, and correct information system flaws.**	**Examine POA&M reports; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); change control records, Work Request, transmittals; records for security-relevant software and firmware updates; other relevant documents to determine if the contractor: - identifies information system flaws; - reports information system flaws; - corrects information system flaws.**		

SI-3 Malicious Code Protection	**1**	**The contractor shall weekly scan the IT assets for malicious code, and identify actions that shall occur in the event malicious code is detected. Possible actions include quarantine of malicious code, eradication, etc.**	**Examine malicious code protection mechanisms; information system configuration settings and associated documentation; other relevant documents to determine if the contractor employs malicious code protection mechanisms and scans the IT assets, used for the IRS contract work, for malicious code, and identifies actions that occur in the event malicious code is detected.**		
SI-3 Malicious Code Protection	**2**	**Virus protection software shall be installed on all workstations, servers, or mobile computing devices.**	**Examine information system virus protection software and verify the software definitions are up-to-date on all workstations, servers, or mobile computing devices used for IRS contract work.**		
SI-3 Malicious Code Protection	**3**	**The virus detection software shall be configured to perform automated updates, and perform automated scanning of all files, incoming and outgoing emails or other network communications.**	**Examine information system virus protection software and verify the software is configured to perform automated updates, and perform automated scanning of all files, incoming and outgoing emails or other network communications.**		
SI-3 Malicious Code Protection	**5**	**Contractors shall not include taxpayer, SBU, or PII information in email messages or attachments without using FIPS 140-2 or later compliant encryption.**	**Examine the contractor email usage policy to ensure that IRS SBU is only sent with approved encryption.**		
SI-3 Malicious Code Protection	**6**	**Personal email accounts shall not be used to conduct any IRS business in performance of the contract.**	**Examine company email policies to ensure that use of an individuals' personal email accounts are prohibited.**		
SI-4 Information System Monitoring	**1**	**The contractor shall employ tools and techniques to monitor events on the information system to detect attacks, vulnerabilities, and detect, deter, and report on unauthorized use of the information system.**	**Examine information system design documentation; information system monitoring tools and technique; information system configuration settings to determine if contractor employs tools and techniques to monitor events on the information system to: detect attacks; vulnerabilities; detect, deter, and report on unauthorized use of the information system.**		
SI-7 Software, Firmware, and Information Integrity	**2**	**The contractor shall enforce explicit rules governing the downloading and installation of software by users.**	**Examine information system configuration settings and associated documentation; incident response records; information audit records; other relevant documents to determine if the contractor incorporates the detection of unauthorized downloading and installation of software. Verify the contractor enforces explicit rules governing the downloading and installation of software by users.**		

SE-1 Inventory of Personally Identifiable Information	**1**	**The contractor is responsible for maintaining an inventory of all PII provided to the contractor, generated by the contractor, or used by the contractor sufficient to enable notification to taxpayers, if disclosed.**	**Examine the inventory list of IRS data, containing PII, maintained by the contractor.**		
SE-2 Privacy Incident Response	**1**	**The contractor shall develop and implement a Privacy Incident Response Plan that provides an organized and effective response to privacy incidents.**	**Examine the Incident Response Plan to determine if PII data disclosure procedures are in place.**		
SE-2 Privacy Incident Response	**2**	**All privacy-related incidents must be reported to the IRS as identified in IR-6, Section 18.6.**	**Examine the Incident Response Plan and determine if it covers procedures on reporting PII data disclosure incidents to SAMC via telephone at (866) 216-4809 (TTY 800-877-8339).**		