3482S	DOA thru August 30, 2025 (Opt. thru 8/2030)							
-----	-----	-----		-----	-----	-----	-----	
		BASIS		Advantage Mailing LLC		GPO		
ITEM		OF		Anaheim, CA		Estimate		
NUMBER	ITEM DESCRIPTION	AWARD		UNIT RATE	COST	UNIT RATE	COST	
--------	----------	-------		----------	----------	----------	----------	
I	PRINTING AND TRIMMING	-----		-----	-----	-----	-----	
1	Certificates							
(a)	Certificates without Variable Data							
1	Make-Ready and/or Setup	18		2500.00	$45,000.00	2000.00	$36,000.00	
2	Running (per 100) copies	80		80.00	$6,400.00	70.00	$5,600.00	
(b)	Certificates with Variable Data							
1	Make-Ready and/or Setup	200		500.00	$100,000.00	750.00	$150,000.00	
2	Running (per 100) copies	950		80.00	$76,000.00	60.00	$57,000.00	
2	Batch Cover Sheets…..per leaf….....	880		10.00	$8,800.00	1.00	$880.00	
II	PACKING FOR DISTRIBUTION	-----		-----	-----	-----	-----	
(a)	Shrink-film packaging… per package	1500		0.50	$750.00	0.50	$750.00	
(b)	Quantities up to 12 lbs., packed in							
	envelopes, cushioned shipping bags, or							
	small shipping containers… per env. bag or container	115		2.50	$287.50	4.00	$460.00	
(c)	Quantities over 12 lbs. up to 32 lbs.,							
	packed in shipping containers… per container	85		15.00	$1,275.00	8.00	$680.00	
	TOTAL				$238,512.50		$251,370.00	
	DISCOUNT			.5%	$1,192.56			
	NET TOTAL				$237,319.94		$251,370.00	
					AWARDED			

U.S. GOVERNMENT PUBLISHING OFFICE

Southeast Region

GENERAL TERMS, CONDITIONS, AND SPECIFICATIONS

For the Procurement of

SPEC Certificates

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

Department of Treasury/IRS

Single Award

TERM OF CONTRACT: The term of this contract is for the period beginning Date of Award and ending August 30, 2025, plus up to four (4) optional 12-month extension periods that may be added in accordance with the "OPTION TO EXTEND THE TERM OF THE CONTRACT" clause in SECTION 1 of this contract.

NOTE: It is anticipated that the period from Date of Award through November 30, 2024 will be a non-production period for setup and security investigative processing tasks with live production beginning December 1, 2024. Live production may begin sooner if setup and security is completed prior to December 1, 2024.

BID OPENING: Bids shall be opened virtually at 11:00 AM, Eastern Time (ET), on August 23, 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 submit 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. To submit a bid, contractor must return a completed "SCHEDULE OF PRICES" which is included at the end of this specification. ***Bids received after the bid opening date and time specified above will not be considered for award.***

BIDDERS, PLEASE NOTE: This is a new term contract. No abstract of previous prices is available.

For information of a technical nature or questions, contact Traci Cobb (404-605-9160 Ext. 4 or tcobb@gpo.gov).

SECTION 1. - GENERAL TERMS AND CONDITIONS

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

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

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

SUBCONTRACTING: The predominant production function for this contract is the printing of the forms (including variable data). Any contractor who cannot perform the predominant production function will be declared non-responsible.

GPO IMPRINT REQUIREMENTS: The GPO imprint requirement, GPO Contract Terms, Supplemental Specifications, 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
(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	Approved PDF Proofs (Page Integrity)
P-10. Process Color Match	Electronic Media

Special Instructions: In the event that PDF proofs are not required by the Government, the following listed alternate standard shall become the Specified Standard:

P-7. Electronic Media

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(s) added under this clause. Further extension may be negotiated under the "EXTENSION OF CONTRACT TERM" clause. See also "ECONOMIC PRICE ADJUSTMENT" for authorized pricing adjustment(s).

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

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

For the purpose of this clause, performance under this contract will be divided into successive periods. The first period will extend from Date of Award and ending August 30, 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 May 31, 2025, 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: Protection of Confidential Information –
(a) The contractor shall restrict access to all information obtained from the IRS in the performance of this contract to those employees and officials who need it to perform the specific services outlined in this contract.

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

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

(d) The contractor shall ensure that each contractor employee with access to IRS work knows the prescribed rules of conduct and that each contractor employee is aware that he/she may be subject to criminal penalties for violations of the Privacy Act.

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

(f) All contractor employees shall either be literate in English or have a translator available at all times who can read, speak, and understand the language in order to ensure all operational, security, and contract requirements are met. The contractor shall ensure communications are provided at a level such that employees can understand instructions and converse with the customer.

(g) Work areas for the production of IRS work shall be in dedicated areas that have fixed barriers and access controlled to only those employees working on IRS work. Signs shall be posted that only assigned employees may enter. All phases of work will be staged in one main area for each process and sufficiently protected from unauthorized access or comingling with non-IRS work. All work areas will be open for IRS representatives at all times. (Refer to Pub 4812 (Rev. 12-2023) sections MP-1, MP-2, and PE-3 (https://www.irs.gov/pub/irs-pdf/p4812.pdf).

(h) At least one supervisory employee must be permanently assigned to the secured areas to visually observe at all times the printing, imaging, binding, construction, inserting, storing, shipping, and destruction of any spoiled materials.

SENSITIVE BUT UNCLASSIFIED (SBU) 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 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 to the IRS, as early as 24 hours, but no later than 72 hours, after award.

(c) Depending upon the nature of the type of investigation necessary, it may take a period up to 11 months to complete complex personnel screening investigations. At the discretion of the Government, background screening may not be required for employees with recent or current favorable Federal Government investigations.

(d) To verify the acceptability of a non-IRS, favorable investigation, the contractor shall submit the same forms or information needed, as specified in paragraph (b) above, for each such employee in compliance with instructions to be furnished to the IRS, as early as 24 hours, but no later than 72 hours, after award.

(e) 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 IRS 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.

(f) The contractor shall immediately notify the Contracting Officer and the IRS 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.

SECURITY OF INFORMATION AND MATERIALS: 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 SBU data must be adequately protected and secured and meet the required physical security minimum protection standards as defined in Publications 1075 (https://www.irs.gov/pub/irs-pdf/p1075.pdf) and 4812 (https://www.irs.gov/pub/irs-pdf/p4812.pdf). Unless otherwise indicated herein, all extra copies, materials, waste, etc., must be destroyed in accordance with IRS Publications 1075 and 4812, Tax Information Security Guidelines for Federal, State, and Local Agencies.

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 1075 and 4812, 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 1075 and 4812, Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities (as revised) 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.

(b) All IRS systems that handle or process Federal Tax Information or other Sensitive But Unclassified information, including 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.

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).

Contractors 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. Authorized contractor employees shall apply, authenticate, and retrieve a digital certificate.

2. Data Tracking and Accounting: Contractors 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 contracted entity is a federal, state, or local agency and transmitted data contains FTI, these procedures shall meet the requirements of Publications 1075 and 4812.

3. All contractors 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 acknowledgement of receipt of SBU information.

4. Data Transfer Log File: Contractors 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 is possible.

5. Confirmation of Successful Data Transfers and Record Count: When a contractor receives a file from the IRS via SFTP or SecureZip™, 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 contact the IRS (Eugenia Collins (Eugenia.F.Collins@irs.gov) and/or the publishing specialist listed on the print order) immediately and request that the file be retransferred. Requests for retransfers 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.

6. Sensitive But Unclassified 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 GPO (Traci Cobb, tcobb@gpo.gov, 404-605-9160 x4), the IRS Contracting Officer Representative (Eugenia Collins, Eugenia.F.Collins@irs.gov, 470-769-2003), and the Computer Security Incident Response Center (CSIRC) Incident Response Operations Team at (240) 613-3606. The 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.

7. 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 1075 and 4812.

8. 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.

9. 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.

10. Safeguard Disclosure of Federal Taxpayer Information Data Transmitted Through the Secure Data Transfer: 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 the 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.

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

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

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 Atlanta 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 IRC section 6103(p)(4) and (p)(7)).

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/SECURITY CLAUSES: In conjunction with the Privacy Act of 1974, contractors must ensure that all employees review Privacy Awareness Training, made available by IRS' Office of Privacy, before gaining access to any sensitive but unclassified data (SBU). In addition, the contractor must comply/abide by the IRS Acquisition Security clauses (see Exhibits A through I).

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.

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.

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

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

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.

PRE-AWARD SECURITY INFORMATION AND PRODUCTION PLANS: Contractor must complete and submit the below items to the IRS within two (2) workdays after Government request.

- A copy of any internal security review and findings the contractor may have made within the previous 12 months;
- A narrative description of the contractor's proposal to comply with required security measures;
- A copy of all the contractor's policies and procedures relating to security;
- An organization listing or chart;
- Contractor's Production Plans (written, detailed copies of each of the plans listed below);
- Physical Security and Cyber Security Self-Assessments (see below);

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, or mutilated items. The plans shall detail the actions to be taken by the contractor when defective, missing, or mutilated items are discovered. These actions must be consistent with the

requirements found in GPO Contract Terms GPO 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 to ensure that the production and delivery of the products in this contract meet specifications and Government requirements. This includes maintaining 100% accountability in the accuracy of imaging 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, or mutilated 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 documenting 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 relationship 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.

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, and all outgoing materials cleared for shipment.

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 on 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 must address, at a minimum, the following:

(a) Materials – How all accountable materials will be handled throughout all phases of production. This plan shall also include the method of disposal of all production waste materials.

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

    Items with variable data must be stored in locked areas.

    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.

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 and PDF file formats. Contractor must submit the completed self-assessments in conjunction with the production plans.

These documents will be reviewed and analyzed by both Physical Security and Cyber Security and any other security components, if implicated, for completeness, accuracy, and compliance to 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.

The contractor may contact Traci Cobb (tcobb@gpo.gov) or Eugenia Collins (Eugenia.F.Collins@irs.gov) with 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.

THE SECURITY INFORMATION AND PROPOSED PLANS ARE SUBJECT TO REVIEW AND APPROVAL BY THE GOVERNMENT AND AWARD WILL NOT BE MADE PRIOR TO APPROVAL OF SAME. ANY OR ALL OF THESE PLANS MAY BE WAIVED AT THE DISCRETION OF THE GOVERNMENT.

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 REVISED PLANS ARE SUBJECT TO GOVERNMENT APPROVAL. The revised plans must be submitted to GPO within two (2) 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.

PRE-AWARD AND POST-AWARD TELECONFERENCE CALLS: The contractor will be contacted to set up several teleconference calls.

Pre-Award Call (estimated 1-1/2 hours) – IRS Cybersecurity and Physical Security will provide the contractor with necessary forms and expectations leading up to the 1-hour post-award call 3 (see below).

Post-Award 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.

Post-Award 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.

Post-Award Call 3 (estimated 1 hour call prior to the three-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.

Post-Award Call 4 (estimated 1-1/2 hours) – The purpose of the conference call will be to discuss and review the requirements of the contract. Project-specific information will be reviewed. Representatives from the Internal Revenue Service Survey Team, the Government Publishing Office, and the Marketing Research Firm (if applicable) will attend this call.

To establish coordination of all required operations, the contractor must have a representative from each involved production area in attendance for the calls.

POST-AWARD CONTRACTOR SECURITY MANAGEMENT: The IRS requires that the contractor's employees having a need for staff-like access to SBU information must be approved through an appropriate level of security screening or investigation. Immediately upon award, the contractor must furnish the Government with a description of all positions requiring staff-like access to IRS data (files or on the printed product). The Government (including an IRS personnel security officer) will assess the risk level for each position and determine the need for individual security investigations.

Upon award of contract, the IRS will provide the necessary forms and instructions to the contractor. Within 24 hours of receipt of the forms/instructions, the contractor must return the forms filled out for each employee who will be involved in the production on this contract. The contractor must comply/abide by the following IRS Acquisition Security clauses (see Exhibits A through I).

- IR1052.204-9000-Submission of Security Forms and Related Materials.
- IR1052.204-9001-Notification of Change in Contractor Personnel Employment Status, Assignment, or Standing.
- IR1052.204-9002-IRS Specialized Information Technology (IT) Security Training (Role-Based) Requirements.
- IR1052.209-9002-Notice and Consent to Disclose and Use of Taxpayer Return Information.
- IR1052.224-9000-Safeguards Against Unauthorized Disclosure of Sensitive but Unclassified Information.
- IR1052.224-9001-Mandatory IRS Security Training for Information Systems, Information Protection and Facilities Physical Access.
- IR1052.239-9008-Information Systems and Information Security Controls for Contracting Actions Subject to Internal Revenue Manual (IRM) 10.8.1.
- IR1052.239-9009-Information Systems and Information Security Controls for Contracting Actions Subject to IRS Publication 4812.
- IR1052.239-9010-Information System and Information Security Control Standards and Guidelines Applicability.

Contractor personnel requiring investigation will not be allowed staff-like access to IRS data until approved by the IRS National Background Investigation Center (NBIC). The IRS shall bear the cost of conducting a security screening for contractor employees requiring one. Other employees will be screened on an "as needed" basis. All employees will receive a moderate level security clearance initially, which may be raised, as applicable, if deemed necessary by the IRS at any time during the contract.

All applicable employees must be fingerprinted. Fingerprinting must be done at a GSA Credentialing Station. When the employee receives an email in reference to fingerprinting, the employee shall schedule an enrollment appointment. Any costs for fingerprinting not conducted at an approved credentialing location will be borne by the contractor. Travel to and from the credentialing office will be borne by the contractor.

Contractor must ensure that all contractor employees who require staff-like access to IRS information or information systems (where these are located at contractor managed facilities using contractor managed assets), regardless of their physical location, complete the required Privacy Training and Security Awareness Training prior to being granted access to SBU data. The IRS will forward training material upon award of the contract.

Contractor employees who will have physical and/or logical access to IRS taxpayer data must be both eligible and suitable to work on an IRS contract as determined by IRS Personnel Security. Contractor is responsible for providing the following forms/documentation for their employees assigned to IRS contracts to IRS Personnel Security:

Eligibility Requirements include the following:
Any employee who is foreign-born must provide proof of U.S. citizenship or Lawful Permanent Resident status. Employees must provide their Alien Registration Number ("A" number) for corroboration by IRS Personnel Security:

1. Subjects must be federal tax compliant and must remain tax compliant while actively working on IRS contracts. IRS will check subjects' tax compliance status upon notification of subject being assigned to work on the IRS contract.

2. All male subjects born after December 31, 1959, must be registered with Selective Service (SS). For male U.S. citizens, proof of registration can be obtained by accessing the SS website at https://www.sss.gov/ and following the prompts on the "Verify or Update Registration" tab. If the search results in a "Matched Record," click on the "*Print an Official Selective Service Registration Acknowledgment Letter"* button and follow the prompts for saving the letter as a PDF file. The letter should then be provided to IRS Personnel Security. If the subject is not registered, he must provide a waiver of registration requirement from SS.

Suitability Requirements include the following:

- Two completed Form 14606 Risk Assessment Checklist (IT RAC and Non-IT RAC) spreadsheets. The spreadsheets will be completed by the contractor point of contact to provide needed information about each employee who will be handling variable data (data files or on the printed product) on the contract.
- OPM's Position Designation Tool (PDT). The contractor will be required to provide position titles and position descriptions for each employee who will be handling variable data (data files or on the printed product) on the contract.

The following forms will be supplied by the Government and must be completed by each employee assigned to the contract:

1. A completed and signed OF-306, *Declaration for Federal Employment*
2. A signed Form 15269 (English or Spanish as applicable), *Conditional Access to Sensitive Information Non-Disclosure Agreement*
3. A signed Form 13340, *Fair Credit Reporting Act*
4. Review and initial Notice 1379, *Tax Record Check Notice*
5. A completed National Background Investigation Services (NBIS) Electronic Application for Investigations Processing (APP) package. The IRS Personnel Security will send each subject a separate email with instructions for completing APP. The APP package is only required for those subjects who do not have a favorably adjudicated federal background investigation within the last five (5) years.

The IRS Human Capital Office, Personnel Security, Contractor Security Onboarding office may request additional forms to complete their investigation.

Contractor must complete mandatory briefings known as Security Awareness Training (SAT). The IRS Contracting Officer's Representative (COR) shall provide soft copy versions of each briefing.

Upon completion of the briefings, the following certification forms must be submitted to Eugenia Collins (Eugenia.F.Collins@irs.gov):

- Form 11370, Certification of Annual UNAX Awareness Briefing
- Form 14616, Contractor Security Awareness Training (SAT) Certification

Contractor must return training certifications to IRS within 5 business days of receiving the Personnel Security's memo approving interim or staff-like access to Eugenia Collins (Eugenia.F.Collins@irs.gov). If additional/newly hired employees will work on the contract, the training certificates are due 10 days after interim staff-like access approval. The training is due annually to the IRS on October 31st. See clause IR1052.224-9001 (Exhibit F).

Specialized Information Technology Security (SITS) training is required for some employees. Internal Revenue Manual 10.8.1.4.2.2 requires prospective contractor employees to complete specialized role-based training prior to beginning duties related to their specialized IT security role(s) under the contract. The SITS training is due annually to the IRS on June 1st. See clause IR1052.204-9002 (see Exhibit C).

The contractor is responsible for any costs incurred to meet the specialized role-based training requirements or the contractor has the option to take the required number of hours for each specialized role on the following website at no cost: https://fedvte.usalearning.gov.

The following form must be completed by the contractor to separate an employee/contractor from an IRS contract: Form 14604, *Contractor Separation Checklist* (to be provided upon request).

The contractor shall email the Form 14604 to Eugenia Collins (Eugenia.F.Collins@irs.gov) and the Contracting Officer within one (1) workday of the contractor becoming aware of any change in the employment status, information access requirement, assignment, or standing of a contractor employee under this contract or order.

ASSIGNMENT OF JACKETS, PURCHASE AND PRINT ORDERS: A GPO jacket number will be assigned, and a purchase order issued to the contractor to cover work performed. The purchase order will be supplemented

by an individual 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 August 30, 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 for the period specified herein. Shipment/delivery of items or performance of work shall be made only as authorized by orders issued in accordance with the clause entitled "ORDERING." The quantities of items specified herein are estimates only and are not purchased hereby. Except as may be otherwise provided in this contract, if the Government's requirements for the items set forth herein do not result in orders in the amounts or quantities described as "estimated," it shall not constitute the basis for an equitable price adjustment under this contract.

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

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

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

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

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

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

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

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

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

Invoices may also be mailed to: U.S. Government Publishing Office, Office of Financial Management, Attn: Comptroller, Stop: FMCE, Washington, DC 20401.
NOTE: Vendors are expected to submit invoices within 30 days of job shipping/delivery.

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/agency/billing-and-payment.

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

On the same day the billing invoice is submitted to GPO for payment, the contractor is to email a copy of the invoice and all supporting documents to the IRS contact listed on the print order. The requisition number, program number, print order number, and form number shall be noted on the billing documents.

SECTION 2. - SPECIFICATIONS

SCOPE: These specifications cover the production of face only forms (certificates and batch cover sheets) requiring such operations as electronic prepress, proofing, printing, variable imaging, trimming, packing, and distribution. Currently, there are 18 different versions of the certificates.

TITLE: SPEC Certificates

QUANTITY:

Certificates without Variable Data: Quantities will range from approximately 75 copies to approximately 4,500 copies per order.

Certificates with Variable Data: Quantities will range from approximately 10 copies to approximately 5,000 copies per order.

Batch Cover Sheet: Quantities will range from approximately 10 copies to approximately 50 copies per order of certificates with variable data. No batch cover sheet is required for orders of certificates without variable data.

FREQUENCY OF ORDERS:

Certificates without Variable Data: Approximately 18 orders will be issued per year. Several orders may run concurrently.

Certificates with Variable Data including Batch Cover Sheet: Approximately 200 orders will be issued per year. Several orders may run concurrently.

NUMBER OF PAGES:

Certificates without Variable Data: Face Only

Certificates with Variable Data: Face Only

Batch Cover Sheet: Face Only
Note: Batch Cover Sheets may be multiple face only leaves depending on the number of certificates ordered on the print order.

TRIM SIZES:

Certificates without Variable Data: 11 x 8-1/2" or 8-1/2 x 11"

Certificates with Variable Data: 11 x 8-1/2" or 8-1/2 x 11"

Batch Cover Sheet: 11 x 8-1/2"

EXHIBITS: Exhibits A through I are representative of the requirements which will be required under this contract. The most current version of the below forms will be used. It cannot be guaranteed that forms for future orders will correspond exactly to these exhibits.

- Exhibit A: IR1052.204-9000-Submission of Security Forms and Related Materials.
- Exhibit B: IR1052.204-9001-Notification of Change in Contractor Personnel Employment Status, Assignment, or Standing.
- Exhibit C: IR1052.204-9002-IRS Specialized Information Technology (IT) Security Training (Role-Based) Requirements.
- Exhibit D: IR1052.209-9002-Notice and Consent to Disclose and Use of Taxpayer Return Information.
- Exhibit E: IR1052.224-9000-Safeguards Against Unauthorized Disclosure of Sensitive but Unclassified Information.

- Exhibit F: IR1052.224-9001 Mandatory IRS Security Training for Information Systems, Information Protection and Facilities Physical Access.
- Exhibit G: IR1052.239-9008-Information Systems and Information Security Controls for Contracting Actions Subject to Internal Revenue Manual (IRM) 10.8.1.
- Exhibit H: IR1052.239-9009-Information Systems and Information Security Controls for Contracting Actions Subject to IRS Publication 4812.
- Exhibit I: IR1052.239-9010-Information System and Information Security Control Standards and Guidelines Applicability.

GOVERNMENT TO FURNISH: Electronic media will be furnished as follows –

Platform: Microsoft Windows (current or near current version)

Storage Media: Print files, dummy data, and data files will be available via email or for download from a Government-hosted SFTP service. Appropriate log-on instructions and protocol will be provided by the Government at time of award.

Software: Adobe Acrobat, Adobe InDesign, and Zipped Microsoft Excel (current or near current versions).

All platform system and software upgrades (for specific applications) which may occur during the term of the contract must be supported by the contractor.

Fonts: All fonts will be Embedded and/or Embedded Subset (PDF) or furnished (InDesign) for the print files**.**

Colors: May be identified as one or more of the following: RGB, CMYK, Black, and/or Pantone/Spot colors. If necessary, contractor to convert all colors to CMYK for the Certificates and to spot color Black for the Batch Cover Sheet.

Additional Information: The base image of the various certificates will be provided via Adobe Acrobat and InDesign. If necessary, contractor to create the bleeds.

Dummy data files to be used for proofing purposes will be supplied on the initial print order for each certificate.

The recipient names and shipping addresses for the certificates printing with variable data will be provided in an Excel spreadsheet. The spreadsheet will be used to pull the recipient name for the variable data and will print as the Batch Cover Sheet.

The size of the recipient name may need to be adjusted to ensure the entire name prints in the allotted space.

The spreadsheet (Batch Cover Sheet) may need to be manipulated to print landscape with all columns set to fit on one page. Batch Cover Sheets may be multiple face only leaves depending on the number of certificates ordered on the print order.

Form 6153 (IRS Carton Label with labeling and marking specifications for shipping containers to be completed ELECTRONICALLY for each destination) will be emailed to the contractor. See "PACKING AND LABELING" for additional requirements.

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

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 required to have Adobe Acrobat 7.0 Professional (or more recent) software (not Adobe Reader) and the capability to receive via email and open file attachments compressed into a SecureZip™ file format.

The contractor must take the data and format it to produce all the required information using their own equipment. It is the contractor's responsibility to ensure that the imaging equipment used on this contract has the capability to image all required areas.

The contractor must appoint a Project Manager to oversee the contract from beginning to end. The contractor must provide the name, email, and phone numbers of the Project Manager and the core team to GPO and the IRS.

Responsibility for Inspections and Tests: The contractor is responsible for any inspections and tests required to ensure that the products ordered under this 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 production run. Contractor must develop and submit prior to award a quality assurance checklist (see "Quality Control Plan") for all components of the production process.

Contractor's Records: The contractor shall maintain records of all inspections and tests performed on the products ordered under the contract. The contractor shall save and preserve all records of these inspections and tests for a minimum of 120 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.

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 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 file, and any errors, media damage or data corruption that might interfere with proper file image processing. All problems with furnished media must be reported within three (3) hours of receipt to the IRS contact listed on the print order and to GPO Southeast, Traci Cobb (tcobb@gpo.gov).

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

High resolution output (as indicated under "ACCEPTABLE PRINTING METHODS") required for printing.

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

PROOFS: Soft proofs(*) will be required on the initial print order for each certificate.

(*) PDF Proofs: "Press Quality" PDF Proofs will be emailed to the agency contact listed on the print order. The proofs must utilize the furnished dummy data which usually consists of one record. Proofs must include all variable data that will print on the final product.

All PDF proofs are for content only and must be created using the same Raster Image Processor (RIP) that will be used to produce the final printed product. Proofs must show color and contain all crop marks. These proofs will not be used/approved for color match or resolution.

Contractor must call the IRS contact listed on the print order to confirm receipt.

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

Contractor must not print prior to receipt of an "OK to print" via email from the agency. Contractor furnished proof approval letters will not be recognized for proof approval/disapproval. Only GPO generated proof letters will be recognized for proof approval/disapproval.

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.

Certificates without Variable Data: White Gloss-Coated Cover, Basis Weight: 80 lbs per 500 sheets, 20 x 26", equal to JCP Code L10.

Certificates with Variable Data: White Gloss-Coated Cover, Basis Weight: 80 lbs per 500 sheets, 20 x 26", equal to JCP Code L10.

Batch Cover Sheet: White Bond, Basis Weight: 20-24 lbs per 500 sheets, 17 x 22", equal to JCP Code G10.

PRINTING:
Certificates without Variable Data: Certificates print tints/solids with reversing, type, and rule matter via 4-color process on the face only.

Certificates with Variable Data: Certificates print tints/solids with reversing, type, and rule matter via 4-color process with variable data (recipient name) printing in Black on the face only.

Batch Cover Sheet: Cover Sheets prints type and rule matter in Black on the face only.

The GPO imprint is waived and must not print on the finished products.

ACCEPTABLE PRINTING METHODS:
Certificates without Variable Data: Forms must be printed via offset printing on a minimum 4-color press with one single pass. Forms (i.e. ink) MUST be compatible for usage with a high heat laser printer. No smearing, lifting, or loss of images due to use with a laser printer will be accepted.

Certificates with Variable Data: At contractor's option, the product may be produced via conventional offset or digital printing provided Quality Level III standards are maintained. Final output must be water-resistant ink or toner with a minimum of 175-line screen. Output must be at a minimum resolution of 2400 x 2400 dpi or 1200 x 1200 dpi x 8 bit plus a RIP that provides an option for high quality color matching such as Device Links Technology and/or ICC Profiles. Resolution that is enhanced or simulated by software will not be acceptable. NOTE: Contractor must produce the entire job either conventional offset or digital printing; split production methods are not acceptable without prior approval.

Batch Cover Sheet: Xerographic reproduction/copying or direct imaging is acceptable.

MARGINS:
Certificates without Variable Data: Full and/or uncommon bleed on all dimensions.

Certificates with Variable Data: Full and/or uncommon bleed on all dimensions.

Batch Cover Sheet: Adequate gripper.

TRIMMING:
Certificates without Variable Data: Trim four sides.

Certificates with Variable Data: Trim four sides.

Batch Cover Sheet: Trim four sides.

PACKING AND LABELING:
Certificates without Variable Data: Shrink-wrap in suitable units with one piece of same size (8-1/2 x 11") chipboard or equal on the bottom of each shrink-wrapped package. Destinations receiving less than 50 copies do not require shrink-wrapping. Shipments must be packed in the quantity listed on the print order*. If no quantity is provided, shipments must be packed in UNIFORM quantities per carton*. *Contractor must NOT deviate from the specified quantity.

Certificates with Variable Data including Batch Cover Sheet: Shrink-wrap in suitable units with one piece of same size (8-1/2 x 11") chipboard or equal on the bottom of each shrink-wrapped package. Destinations receiving less than 50 copies do not require shrink-wrapping. Place the Batch Cover Sheet on top of the contents of each package.

All cartons must be packed solid with a maximum weight of 32 lbs per carton. Pack solid in corrugated or solid fiber shipping containers, bursting strength: 200p.s.i, minimum. Carton bottoms may be glued, stapled, or sealed with polyester tape (2 to 3 inches width, not reinforced), minimum 12kNm (65 lbs./inch) traverse tensile strength. If stapled, the cartons may only be stapled on the bottom and/or side; no staples are to be used on top. Cartons are to be sealed at the top with paper or polyester tape (2 to 3 inches width, not reinforced). Contractor will determine exact dimensions of carton in accordance with folded and/or trim size and weight of the product produced. Cartons must not exceed 17-1/2" (L) x 11-1/2" (W) x 9" (D) in exterior dimensions. NOTE: Packing peanuts/beads are not acceptable carton fillers.

*In some cases, there may be one carton with an odd quantity due to the quantity packed per carton not dividing equally in the quantity ordered. The label for that single carton MUST be labeled accurately with the carton quantity (see CARTON LABELING for electronically correcting label quantity). Place that odd carton at the top of the load.

CARTON LABELING: Contractor must reproduce shipping carton label at 100% on white paper from furnished PDF file, fill in appropriate fields and securely attach one label to each carton. NOTE: Carton labels contain barcodes; therefore, dot matrix printing is NOT acceptable.

All cartons must have IRS Shipping label affixed to one carton end only (never top, long side, or bottom). On cartons shipped via small package carrier (SPC), affix the SPC label on top of carton on the end nearest to IRS label. On small package carrier (SPC) boxes/envelopes, the IRS label is to be affixed to the top of each package and the SPC shipping label to the reverse side of the package (this includes advance distributions and IRS samples). All shipments to IRS National Distribution Center via SPC are to leave "To (Consignee) Address" field blank. Correct labeling of shipping cartons, in strict accordance with the requirements of these specifications, is essential to the identification, distribution and warehousing activities of the IRS. Use of any other label is prohibited and may be cause for rejection of reimbursement for any expenses incurred to correct use of improper labels.

The following must be updated ELECTRONICALLY by the contractor, when not entered by IRS on the PDF label using Adobe Acrobat 7.0. DO NOT MAKE HAND-WRITTEN UPDATES TO THE LABEL UNDER ANY CIRCUMSTANCES.

--Carton # of #
--From Address
--To Address

--Carton Quantity

If requested, the contractor must send an electronic PDF proof of label prior to reproducing.

FAILURE OF THE CONTRACTOR TO COMPLETE THE PDF LABEL ELECTRONICALLY WILL RESULT IN THE SHIPMENT BEING REJECTED AND RE-LABELED AT THE CONTRACTOR'S EXPENSE.

If a "0" is pre-filled in on the furnished PDF label, then contractor MUST change the "0" to reflect actual quantity inside cartons. Contractor must ensure that all cartons have the same quantity. The carton count field in the PDF file is directly linked to the barcode field; therefore, the contractor must press "enter" or "tab" after entering the quantity in order for the quantity to be reflected in the barcode. All changes to the carton count field MUST be made in the electronic label (not hand filled in) to whatever the true carton quantity is so that it is reflected on the label in both the quantity and barcode fields. NOTE: In the case of one carton with an odd quantity due to the quantity packed per carton not dividing equally into the quantity ordered, the label for that single carton must also be updated electronically to reflect the true quantity per carton.

Automated "Carton # of #" fields: To print the correct number of labels for each address with sequential carton numbers, input in the total number of cartons and press "Print Labels" button. Warning: Once the print button is pressed, printing cannot be canceled. Be sure all information is correct prior to printing labels.

PACKAGING AND PACKING PROBLEMS: In addition to other inspection procedures detailed elsewhere in these specifications, the contractor is responsible for correcting all packaging and packing problems (i.e., mislabeled cartons, IRS carton labels not being used or securely attached, cartons not being packed solid, incorrect pallets, or pallets not being layered correctly). The delivery will either be returned to the contractor to be corrected or the contractor may be billed by GPO for the amount that accrued in fixing the problem by an outside vendor.

"Mislabeling" means any error on the carton label, which incorrectly states or identifies the title of the form; the form identification number; or the quantity of forms contained in the carton, or has any missing information, or is not securely attached.

DISTRIBUTION: All shipments are f.o.b. contractor’s city. Complete addresses and quantities will be furnished with the print orders. Certificates with variable data will ship to approximately 50 addresses per print order. Certificates without variable data will ship to approximately 3 addresses per print order.

The following information applies to all F.O.B. Contractor's City shipments:
- All consignments weighing less than 750 pounds must be shipped GROUND via a furnished IRS Small Package Carrier (UPS) account number. If the contractor does not have such an account, the IRS will establish one for the contractor upon award of the contract. Contractor must not use their own small package carrier account.

NOTE: The contractor must have the capability to generate the Small Package Carrier shipping labels electronically. Each label must provide the following 2 reference fields: Reference Field 1 - GPO Jacket Number; Reference Field 2 - IRS Requisition Number.

The contractor cannot be reimbursed for using his or her own small parcel carrier account and/or BL's, nor may GPO GBL's be cut for this order.

Contractor must notify the ordering agency on the same day that the product ships via email to the IRS contact(s) cited on the print. The subject line of this message shall be "Distribution Notice for Program 3482-S, Print Order XXXXX". The notice must provide all applicable tracking numbers, shipping method, and title. Contractor must be able to provide copies of all shipping receipts upon agency request.

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).

No definite schedule for placement of orders can be predetermined. The following schedule begins the first workday after notification of availability of print order and furnished materials; the workday after notification will be the first workday of the schedule.

- It is anticipated that the majority of the orders will be placed during February and March.
- Contractor must complete production and ship within 10 workdays.
- No specific date is set for submission of proofs. Proofs must be submitted as soon as possible to allow for revised proofs if contractor's errors are judged serious enough to require them. Proofs are required only on initial print order for each certificate.
- Proofs will be withheld no more than 2 workdays from their receipt at the ordering agency until approval/disapproval from the agency via email.
- All proof time (initial print order only) is included in the 10 workdays schedule.

The ship/deliver date indicated on the print order is the date products ordered f.o.b. contractor's city must be made available to the small package carrier service indicated by the IRS.

Contract Closeout: Within 30 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.

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

For compliance reporting purposes, the contractor must notify the U.S. Government Publishing Office of the date of shipment. Upon completion of each order, contractor must email the GPO Southeast Region (infosoutheast@gpo.gov) and the Shared Support Services Compliance Section (compliance@gpo.gov). The subject line of this message shall be "Distribution Notice for Program 3482-S, Print Order XXXXX, Jacket Number XXX-XXX.". The notice must provide all applicable tracking numbers and shipping methods. Contractor must be able to provide copies of all shipping receipts upon request.

SECTION 3. - DETERMINATION OF AWARD

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

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

			(1)	(2)
I.				
	1.	(a)	18	80
		(b)	200	950
	2.	880		

II.

(a) 1500
(b) 115
(c) 85

This page is intentionally blank.

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 quotes, may be declared nonresponsive.

An entry of NC (No Charge) shall be entered if bidder intends to furnish individual items at no charge to the Government.

Bids submitted with NB (No Bid), NA (Not Applicable), or blank spaces for an item will 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 invoices must be itemized in accordance with the line items in the "SCHEDULE OF PRICES."

I. PRINTING AND TRIMMING: Prices offered shall include the cost of all required materials and operations necessary (including proofs when required) for the complete printing and trimming of the product(s) listed in accordance with these specifications.

	Make-ready and/or setup (1)	Running Per 100 copies (2)
1. Certificates:		
(a) Certificates without Variable Data	$_____	$_____
(b) Certificates with Variable Data	$_____	$_____
2. Batch Cover Sheets …… per leaf	$_____	

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

(a) Shrink-film packaging ..... per package ..... $_____

(b) Quantities up to l2 lbs., packed in envelopes, cushioned shipping bags, or small shipping containers ..... per envelope, bag, container. $_____

(c) Quantities over 12 lbs. up to 32 lbs., packed in shipping containers ..... per container ..... $_____

_____
(Initials)

SHIPMENT(S): Shipments will be made from: City _____, State _____

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

DISCOUNTS: Discounts are offered for payment as follows: _____ Percent, _____calendar days. See Article 12 "Discounts" of Solicitation Provisions in GPO Contract Terms (Publication 310.2).

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

BID ACCEPTANCE PERIOD: In compliance with the above, the undersigned agree, if this bid is accepted within_____ calendar days (60 calendar days unless a different period is inserted by the bidder) from the date for receipt of bids, to furnish the specified items at the price set opposite each item, delivered at the designated points(s), in exact accordance with specifications.

NOTE: Failure to provide a 60-day bid acceptance period may result in expiration of the bid prior to award.

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

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

_____
(Street Address)

_____
(City – State – Zip Code)

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

_____
(Person to be Contacted) (Telephone Number) (Email)

THIS SECTION FOR GPO USE ONLY

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

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 sensitivebut 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 properlybadged);
- Possess login credentials to information systems (internal or external systems thatstore, 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/orinterpret) 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. Fordetails 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 uponrequired completion of a favorable suitability/fitness determination conducted by IRS Personnel Security.

For security requirements at contractor facilities using contractor-managed resources, pleasereference 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 followingeligibility/suitability pre-screening criteria, as applicable:

- IRS account history for federal tax compliance (for initial eligibility, as well asperiodic 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 theSelective 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 backgroundinvestigations.

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/agreementand 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 andthe COR.

Contract Duration:

a. Contractor (including subcontractor) personnel whose duration of employment is180 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, SelectiveService 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 contractorwho 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/orSBU 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 ProvidingProtection; 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 ofIRS 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 asubcontractor, at any tier, the same Federal Acquisition Regulation (FAR) and local security or safeguard clauses or provisions for protecting SBU information or information systems thatapply 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 Securitywithin one (1) business day of the contractor (including subcontractor) becoming aware of anychange in the employment status, information access requirement, assignment, or standing ofa 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 thegaining 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 figureprominently 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 securitydocuments 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 routinelyworks 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 FurnishedEquipment (GFE), or Government Furnished Information (GFI) (to include PersonalIdentity 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 offederal workspace that is vacant.

As a rule, the change in the employment status, assignment, or standing of a contractor (orsubcontractor) personnel to this contract or order would not form the basis for an excusabledelay 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 2021)

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 OL5081 process or 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 Security System Management 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 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)

IR1052.209-9002 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:

_____ [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:

_____ [OFFEROR NAME]

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

_____
[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]

Offeror Taxpayer Identification Number: _____

Offeror Address: _____

Name of Individual Executing Consent: _____

Title of Individual Executing Consent: _____

Signature: _____

Date: _____

IR1052.224-9000 Safeguards Against Unauthorized Disclosure of Sensitive butUnclassified Information (JUN 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 orforeign policy.' SBU may be categorized in one or more of the followinggroups—
   - Federal Tax Information (FTI), including any information on or related to a taxreturn
   - Returns and Return Information
   - Sensitive Law EnforcementInformation
   - Employee and Personnel Information
   - Personally IdentifiableInformation (PII)
   - Information Collected or Created fromSurveys
   - Other ProtectedInformation
2. Confidentiality requirements for tax returns and return information (FTI) are established by Section 6103 of the Internal Revenue Code (IRC) (26 USC 6103), and the penalties for unauthorized access and disclosure of returns and return information are found in Sections 7213, 7213A and 7431 of the IRC (26 USC 7213, 7213A and 7431). This contract is covered by IRC 6103(n) and the related regulation - 26 CFR §301.6103(n)-1.
3. Contractors who perform work at contractor (including subcontractor) managed sitesusing 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, ContractorInvestigations, 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 hiredfor 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, andin 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) personnel shall 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 priorwritten approval of the IRS. Requests to make such inspections or disclosures shall be addressed to the CO.
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, eachcontractor (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-likeaccess to SBU information under any IRS contract or order.

7. Training. All Contractor personnel assigned to this contract with staff-like access toSBU 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.

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 incidentmanagement:

   - 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-17Alternate 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 inhardcopy 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) hotlineat (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 orhandle 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 fromthe source material), regardless of form or format, shall be completely purged from all data storage components of the contractor's or subcontractor facilities 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 tomeet 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 Electronic Information Technology, and/or return 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 boundby 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 orappropriate for preservation by that agency or its legitimate successor as evidence ofthe 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 totheir [Agency] contract; and
4. may include deliverables and documentation associated withdeliverables.

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 anddelivered to, or falling under the legal control of, the Government are Federal recordssubject 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 aspermitted by statute orregulation.
3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records createdfor 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. Electronic records and associated metadata must be accompanied by enough technical documentation to permit understanding and use of the records and data.
4. IRS and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not beremoved 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 Liaisonand 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 CFR1230.

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 [Agency] 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 inany 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, andcontrolled unclassified information.

7. The Contractor shall only use Government IT equipment for purposes specificallytied 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-publicIRS 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 deliverablethat contains information covered by the Privacy Act of 1974 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 itdetermines 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, andrequirements 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 beattributed 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 ofthe 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 Training for Information Systems, InformationProtection and Facilities Physical Access (JUN 2021)

The Federal Information Security Modernization Act of 2014 (FISMA) requires each federal agency to provide periodic information security 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 and details that any violation of the Act could result in civil and criminal penalties. Contractor/subcontractor personnelare 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 federalrecords.

1. The contractor must ensure all new contractor/subcontractor personnel complete allassigned 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 would be 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 besubject 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 andneed staff-like access to IRS facilities are required to complete Inadvertent Access to Sensitive Information (SBU) Access training.
   iv. Service Personnel Security 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.

4. Training completion process:

The contractor must submit confirmation of completed SAT mandatory briefingsfor 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 havean IRS network account.

ii. Using the IRS training system which is available to all contractors withIRS 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 personnelcomplete 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, via email, 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 entails staff-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 (JUN 2021)

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. In order 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
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 (JUN 2021)

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:

o Internal Revenue Manual (IRM) 10.8.1 – Information Technology (IT) Security, Policy and Guidance

o IRM 10.5.1 – Privacy Policy, and

o 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 only ☐ Publication 4812 ☐ Both IRM 10.8.1 and PUB 4812

Unless IRS Cybersecurity, (Contract 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)

(See 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 applicable to the immediate contracting action, with due consideration to its proposed approach (and work environment) and standards for applicability described herein, is as follows (check only one):

☐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, or destroyed.

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 the 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) 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 provision)