Jacket: 623-849

Title: TY2021 Information Returns Burden Online Survey

Agency: IRS

Bid Opening: March 22, 2022 at 2:00pm

Contractor Name	Bid	Terms		Discounted Total
BMS Direct, Inc	$18,610.00		days	$18,610.00
Gray Graphics Corp AWARDED	$55,320.00	2.0%	20 days	$54,213.60
Advantage Mailing LLC - Anaheim	$111,780.91	0.5%	20 days	$111,222.01
NPC Inc	$116,374.00	2.0%	20 days	$114,046.52

BID OPENING: Bids shall be opened at 2:00pm, prevailing Eastern Time, on March 22, 2022 at the U.S. Government Publishing Office, Atlanta GA. Due to the COVID-19 pandemic, this will NOT be a public bid opening.

ISSUE DATE: March 14, 2022

ANY QUESTIONS BEFORE AWARD CONCERNING THESE SPECIFICATIONS, CALL (404) 605-9160, EXT. 4 (TRACI COBB).

SPECIFICATIONS

U.S. Government Publishing Office (GPO)
Atlanta Regional Office
3715 Northside Parkway, NW
Suite 4-305
Atlanta, Georgia 30327

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)).

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

Contract Clause 6, "Subcontracts," of GPO Contract Terms (GPO Publication 310.2, effective December 1, 1987 (Rev. 01-18)), is modified to permit subcontracting of the printing of the envelopes.

PRODUCT: Consists of proofing, printing (forms and envelopes), trimming and/or construction, and individualized addressing/mailing of letters. See "QUANTITY" for each individual Item.

Jacket 623-849 will be mailed in 1 wave. The wave will be comprised of 4 "contacts" plus ad hoc mailings. Mailings will begin in October 2022 and continue through January 2023 (see "SCHEDULE"). The first contact of Wave 1 will involve approximately 40,010 taxpayers. The following three contacts will involve this quantity minus the respondents.

SECURITY CLEARANCE: The contractor and all employees who handle variable data (files or on the printed product) must go through an Internal Revenue Service security background investigation. See below requirements:

Requirements for contractors with IRS security clearance or in the process of obtaining IRS security clearance (suitability & background clearance for employees, physical security for production facility, and cyber security for information systems): The contractor will be required to re-validate their clearances as follows (WITHIN TWO WORKDAYS after award):
1. Each contractor employee who handles variable data (files or on the printed product) must complete and sign Form 15269 (English or Spanish as applicable), Conditional Access to Sensitive Information Non-Disclosure Agreement in "Exhibit #3".

2. The contractor must complete and submit two Form 14606 Risk Assessment Checklists (IT RAC and Non-IT RAC). Each RAC will include employees who handle variable data (files or on the printed product).

Requirements for the apparent low bidder if the contractor does not have IRS security clearance nor is in the process of obtaining IRS security clearance (suitability & background clearance for employees, physical security for production facility, and cyber security for information systems): The contractor will be required to complete and submit the following prior to award (WITHIN TWO WORKDAYS after Government notification):
1. A copy of any internal security review and findings the contractor may have made within the previous 12 months;
2. A narrative description of the contractor's proposal to comply with required security measures;
3. A copy of all the contractors' policies and procedures relating to security;
4. An organization listing or chart;
5. Contractor's Security Letter & Plans (see "Exhibit #1" for additional information);
6. Physical and Cyber Security Assessments (worksheets provided by IRS).

In addition, WITHIN TWO WORKDAYS after award, the contractor will be required to submit the following:
1. Each contractor employee who handles variable data (files or on the printed product) must complete and sign Form 15269 (English or Spanish as applicable), Conditional Access to Sensitive Information Non-Disclosure Agreement in "Exhibit #3".
2. The contractor must complete and submit two Form 14606 Risk Assessment Checklists (IT RAC and Non-IT RAC). Each RAC will include employees who handle variable data (files or on the printed product).
3. Each contractor employee who handles variable data (files or on the printed product) must complete and submit all of the security documents listed in “Exhibit #2”.

QUALITY ASSURANCE: The contractor must furnish a complete **Quality Systems Plan** (see below) within FIVE WORKDAYS AFTER AWARD.

Quality Systems: The prime contractor shall initiate, prior to start-up and maintain throughout the term of this contract, Quality Systems to assure conformance to all requirements of this contract. The Quality Systems should be documented in a Quality Systems Plan. The plan should also address what actions will be initiated when defects are detected.

The Quality Systems shall assure the quality of components from subcontractors and subsidiary plants. This element includes assuring that components from different sources will be compatible BEFORE the start of production.

The Quality Systems shall include procedures for assuring that all variable data elements are accurately and completely printed and that all addressed items are mailed.

These procedures shall explicitly describe the methods to be used to assure that no records are missed or duplicated when an interruption of variable printing occurs (e.g., due to equipment malfunction) during all phases of production.

Quality Systems Official: The prime contractor shall designate an official who shall monitor and coordinate the quality system. This official shall serve as the Government's main point of contact on quality matters during the term of the contract. The name of the official shall be provided in the plan along with title, position, and telephone number.

Records: Records of tests, inspections, and critical process controls shall be time stamped and maintained on file. The records must be made available to the GPO and/or IRS inspector until the expiration of the warranty period of this contract (see GPO contract terms). Copies of the forms used to record the inspections and test results shall be submitted with the plan.

All quality control samples must be produced at no additional cost to the Government.

Inspections: The right of the Government to make general or specialized tests and inspections DOES NOT RELIEVE THE CONTRACTOR OF ANY RESPONSIBILITY.

Performance of all elements and functions of the Quality Systems shall not relieve the contractor of responsibility for meeting all requirements in this contract.

Quality Systems Plan: The prime contractor shall submit written outline plans of the Quality Systems and copies of the forms used to record the inspections and test results. The plans shall be emailed to Sylvia Greene (Sylvia.J.Greene@irs.gov) and Traci Cobb (tcobb@gpo.gov). The proposed Quality Systems Plans are subject to Government approval.

SECURE FILE TRANSFER PROTOCOL NETWORK (SFTP) REQUIREMENT: The data files for the mailing addresses will be furnished to the contractor from the Marketing Research Firm (MRF) via Secure File Transfer Protocol network (SFTP). Contractor is responsible for setting up and maintaining a secure network according to the National Institute of Standards and Technology (NIST) SP 800 security guidelines.

POST AWARD CONFERENCE: A post award conference will be held via telephone. The purpose of the conference will be to discuss and review all aspects of the contractor's internal operations required to complete this contract. Representatives from the IRS, GPO, and the Marketing Research Firm will participate in the call. To establish coordination of all required operations, the contractor must have a representative from each involved production area in attendance for the call.

ADDITIONAL POST AWARD TELECONFERENCE CALLS (IF REQUIRED BY IRS PHYSICAL SECURITY AND CYBERSECURITY): The contractor will be contacted to establish several teleconference calls and meetings as specified below. Contractor must make themselves available for calls #1 and #2 below within 1 week after notification.
1) Physical Security initial call (1 hour) – contractor will be given instructions on what supporting documentation needs to be presented to IRS for specific items related to physical security. Supporting documentation will be presented at the Physical Security final meeting (#3) below. Contractor will be allowed 15 workdays from this initial call to assemble supporting documentation. An alternate time frame may be possible if the IRS agrees.

2) Cybersecurity initial call (1 hour) – contractor will be given instructions on what supporting documentation needs to be presented to IRS for specific items related to cybersecurity. Supporting documentation will be presented at the Cybersecurity final meeting (#4) below. Contractor will be allowed 15 workdays from this initial call to assemble supporting documentation. An alternate time frame may be possible if the IRS agrees.

3) Physical Security final review meeting (up to 1 full day) – contractor will present supporting documentation to the IRS for specific items related to physical security. At the government's option, this meeting may be held online or in-person at the contractor's facility. Information will most likely be presented to IRS on WebEx for an online meeting.

4) Cybersecurity final review meeting (up to 3 full days) – contractor will present supporting documentation to the IRS for specific items related to cybersecurity. At the government's option, this meeting may be held online or in-person at the contractor's facility. Information will most likely be presented to IRS on WebEx for an online meeting.

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

IMPORTANT FOR FINAL REVIEW MEETINGS (#3 and #4 above): It is crucial that the contractor have supporting documentation, as specified in the initial call, already prepared and ready for presentation for Physical Security and Cybersecurity final review meetings. If there are high-risk findings from the Physical Security and Cybersecurity final reviews, the contractor will be expected to remediate the high-risk finding in 20 workdays from the final review meeting. An alternate time frame may be possible if the IRS agrees.

ADDITIONAL POST AWARD CALLS (AS NEEDED):
5) IRS Personnel Security call (2 hours) - will discuss the information that is needed from the contractor for each employee working on this contract. Contractor will be allowed 5 workdays from this initial call to assemble required documentation about IT employees that will be working on this contract. Contractor will be allowed 15 workdays from this initial call to assemble required documentation about all other employees that will be working on this contract. An alternate time frame may be possible if the IRS agrees.

6) Production and Quality System review (1 hour) – Production plan and quality system plan 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.

TITLE/FORM NO:
TY2021 Information Returns Burden Online Survey
-- Form 14463 (OS) (12-2021), Catalog Number 74002R

QUALITY LEVEL: III Quality Assurance Through Attributes (GPO Publication 310.1, effective May 1979 (Rev. 09-19)) applies.

QUANTITY: Six (6) individual Items (see below for each Item):
- Item 1: Form (IRS Letter (C1) 6132): 46,013 copies
- Item 2: Form (FAQ (C1) Pub 5578): 46,013 copies
- Item 3: Form (IRS Letter (C2) 6332): 40,013 copies
- Item 4: Form (IRS Letter (C3) 6333): 40,013 copies
- Item 5: Form (IRS Letter (C4) 6334): 40,013 copies
- Item 6: 6 x 9” Window Envelope: 166,043 total copies (see below breakdown)
--160,040 copies print with the indicia
--6,003 copies print without the indicia

NOTE: Contractor to provide bids based on the above quantities per Item. Quantity and price (based on the contractor's rate for each Item) may be adjusted based on actual mailed quantities for Contacts 2, 3, and 4 (Items 3, 4, 5, & 6). Any adjustments in quantity and price will be addressed in a Contract Modification.

TRIM SIZE:
- Items 1, 2, 3, 4, & 5: 8-1/2 x 11” (flat); 8-1/2 x 5-1/2” (folded)
- Item 6: 6 x 9”

PAGES:
- Items 1, 2, 3, 4, & 5: Face Only
- Item 6: Face and Back (before construction)

DESCRIPTION:
Specifications apply equally to each Item unless otherwise specified.

- Items 1, 3, 4, & 5: Face prints type, rule, and/or screen matter in Black with variable data** printing in Black. Variable data includes name and address, date, PIN, and unique number with corresponding barcode.

- Item 2: Face prints type, rule, reverse, and solid matter in Black.

- Item 6: Envelope prints type, rule, line art, and G-48 indicia* in Black ink on the side opposite the seams. Inside of envelope requires a black or blue opaquing security design. Contractor may use his own design, but must guarantee complete opacity and prevent show through of the contents therein. NOTE: All envelopes must conform to the appropriate regulations in the USPS manual for Domestic Mail as applicable.

*NOTE: A plate change is required to print 6,003 copies without the G-48 indicia.

Construction: Open side, side seams, water soluble gummed flap. Die-cut face with one round cornered window, 4-1/2" (w) x 1-3/4" (h), with 4-1/2" (w) dimension parallel to the 9" dimension, at 7/8" from left and 2-1/2" from top edge when viewed with the flap at the top. Cover window with a clear transparent material (glassine or equal) securely glued to all sides of the envelope.

****VARIABLE DATA AND MAIL MERGE**:
- The contractor must take the IRS data and format it to produce all of 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.

- It is critical that the unique number (and its corresponding barcode) furnished on the Excel spreadsheet be matched to its corresponding name, address, and PIN. 100% matching accountability is required.

- It is the responsibility of the contractor to monitor all ID control numbers to ensure that the unique number (and its corresponding barcode) assigned to the individual taxpayer follows that selected taxpayer on all correspondence from initialization to completion of the survey.

- All copies of Items 1, 3, 4, & 5 print with variable data except the copies that deliver to Synavoice (see "DISTRIBUTION").

- Variable imaging is required utilizing data samples furnished in comma delimited text files (.CSV files). All data with the exception of the date will be provided in the data files. Contractor is to use the actual mail date for the date field.

The following merge fields will be clearly indicated in the print files:
-- Date
Notes: 1) The date must be the same font and size as the body of the letter and must align with the right margin.
2) The date will be the actual mail date and will not be included in the data file.

-- Name
-- Address (Address 2) (Address 1) (City) (State) (Zip) (Zip4)
Notes: 1) The name, address and barcode block must be visible through the envelope window.
2) The name & address block must be the same font and size as the body of the letter.

-- Respondent PIN
Note: The PIN must print align with the text.

-- Respondent ID
Notes: 1) When the ID is in barcode format, it should appear in 3 of 9 font. When the ID is human readable, it should have minimum font size of 10, in Arial font.
2) On all Letters, the respondent ID prints above the name and address block with the unique human readable ID to the right of its corresponding barcode.

ACCEPTABLE PRINTING METHODS:
- Items 1 through 5 (excluding variable data if applicable) may be produced via conventional offset or digital printing. Final output must be a minimum of 150-line screen and at a minimum resolution of 1200 x 1200 dpi x 1 bit or 600 x 600 dpi x 4 bit depth technology. Inkjet printing is not acceptable for the shells of these items.
- Item 6 may be produced via conventional offset, digital printing, or flexography. Final output must be a minimum of 150-line screen and at a minimum resolution of 1200 x 1200 dpi x 1 bit or 600 x 600 dpi x 4 bit depth technology.
- Variable data (when applicable) may be printed via digital, laser, and/or inkjet printing.

GOVERNMENT TO FURNISH:
- Purchase Order and print files/manuscript copy (see "ELECTRONIC MEDIA") will be emailed to the contractor upon award.

- One Excel file containing the record layout and the 10 dummy data records (to be used for the proofs with variable data) will be emailed to the contractor upon award.

- Approximately 168,000 total same size (8-1/2 x 11") pre-printed leaves of stock (IRS Letterhead) for Items 1, 3, 4, & 5 (includes make-ready sheets). Paper will deliver to the contractor no later than five business days after award.

- One copy of IRS Form 13456 (IRS Publishing Postage Report) in a fillable PDF file format will be furnished by IRS via email after award - contractor to complete for each mail contact (see "SCHEDULE").

- A total of four Excel files (one for each contact) containing the distribution lists will be uploaded to the Market Research Firm's SFTP site a minimum of five workdays prior to the respective mail dates. The files for contacts 2, 3, and 4 will involve the total quantity minus the respondents. Files will be password protected. Agency will verbally provide password to the contractor after award.

ELECTRONIC MEDIA:

- PLATFORM: Unknown

- SOFTWARE: ADDITIONAL SYSTEM TIME IS REQUIRED. Seven total PDF files (one PDF file for each item and one PDF file for the G-48 manuscript copy) will be provided.
-- Notes for Item 6: 1) Contractor to reset type and rule for the Domestic G-48 indicia and add the indicia to the print file. 2) Window placement in the file may be incorrect. Contractor to create page layout to image as specified (trim size, window placement as indicated in "DESCRIPTION"). 3) Envelopes must conform to the appropriate regulations in the USPS manual for Domestic Mail.

- FONTS: All fonts are Embedded/Embedded Subset.

- COLORS:
-- Items 1, 3, 4, & 5: Identified as Black.
-- Item 2: Identified as CMYK, Black, and Pantone Neutral Black. Contractor to convert all colors to spot color Black.
-- Item 6: Identified as CMYK. Contractor to convert all colors to spot color Black.

- OUTPUT: High resolution output (as indicated under "ACCEPTABLE PRINTING METHODS") required for printing. Variable data requires minimum of 300 dpi.

NOTE: GPO Imprint information does NOT print on any item for this procurement.

ADDITIONAL INFORMATION:
- Contractor must have the ability to edit PDF files (when furnished by the Government).

- Contractor is not to request that electronic files provided be converted to a different format. If contractor wishes to convert files to a different format, the final output must be of the same or higher quality and at no additional cost to the Government.
- The contractor is cautioned that furnished fonts are the property of the Government and/or its originator. All furnished fonts are to be eliminated from the contractor's archive immediately after completion of the contract.
- 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 the finished product.
- Prior to image processing, the contractor shall perform a basic check (preflight) of the furnished media and publishing files to assure correct output of the required reproduction image. Any errors, media damage or data corruption that might interfere with proper file image processing must be reported to your contract administrator.
- The contractor shall create/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.
- When PostScript Files are not furnished - prior to making revisions, the contractor shall copy the furnished files and make all changes to the copy.
- Upon completion of this order, the contractor must furnish final production native application files (digital deliverables) and one "press quality" PDF file with the furnished media. Storage media must be MAC/PC compatible. The digital deliverables must be an exact representation of the final product and shall be returned on the same type of storage media as was originally furnished. The Government will not accept, as digital deliverables, any proprietary file formats other than those supplied, unless specified by the Government.

STOCK: 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.

- Items 1, 3, 4, & 5: JCP Code G45, White 25% Cotton Bond; 50% Recycled, Basis Size 17 x 22", Basis Weight 20#.
Note: The Government will furnish approximately 168,000 total same size (8-1/2 x 11") pre-printed leaves (IRS Letterhead) of stock (includes make-ready sheets). Paper will deliver to the contractor no later than five business days after award.

- Item 2: JCP Code A80, White Opacified Text, Basis Size 25 x 38", Basis Weight 60#
Note: Stock must be smooth finish, 98 brightness (equal in finish and brightness to Domtar Cougar Opaque).

- Item 6: JCP Code V20, White Writing Envelope, Wove Finish, Basis Size 17 x 22", Basis Weight 24#

MARGINS:
- Items 1, 2, 3, 4, & 5: Follow file setup, adequate gripper. When Letters (Items 1, 3, 4, & 5) are folded and inserted into window envelopes, all of the name, address, and barcode block must appear in the window of the envelope. Contractor must perform the "tap test" to ensure that nothing other than this information appears in the window.

- Item 6: All envelopes must conform to the appropriate regulations in the USPS manual for Domestic as applicable*. *See “ELECTRONIC MEDIA” for additional information.

PROOFS: 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. Contractor must not print prior to receipt of an "OK to print" via email.

Soft proofs: The contractor must provide PDF proofs (*) on or before April 8, 2022.

Soft proofs will be withheld not longer than 1 workday from date of receipt by the Government to date of proof approval and/or corrections from the ordering agency via email. NOTE: The date of receipt by the Government is NOT considered the first workday.

(*) Ten (10) "Press Quality" PDF proofs are required for Items 1, 3, 4, & 5. These proofs must utilize the furnished dummy data from the Excel file which consists of ten records and the appropriate mail date as specified in "SCHEDULE". Proofs must include all variable data that will print on the final product (see "DESCRIPTION"). One (1) "Press Quality" PDF proof is required for Items 2, 6 with indicia, and 6 without indicia.

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.

Email the PDF proofs to Sylvia Green (Sylvia.J.Greene@irs.gov) and Traci Cobb (tcobb@gpo.gov). Emails must not exceed 10 MB, so multiple emails may be required. Contractor must call Sylvia Green (470-639-2480) to confirm receipt.

Hard Proofs (upon approval of the PDF proofs): The contractor must provide hard proofs (**) within ten workdays of receiving soft proof approval.

Hard proofs will be withheld not longer than 2 workdays from date of receipt by the Government to date of proof approval and/or corrections from the ordering agency via email. NOTE: The date of receipt by the Government is NOT considered the first workday.

(**) CONTENT/CONSTRUCTION PROOFS: Four digital CONTENT/CONSTRUCTION proofs each of Item 6 (with indicia) & 6 (without indicia) created using the same Raster Image Processor (RIP) that will be used to produce the product. Proof shall be collated with all elements in proper position (not pasted up), imaged face and back, trimmed and folded (constructed) to the finished size/format of the product. Note: Proofs must clearly indicate the size and position of the window.

(**) PRIOR-TO-PRODUCTION SAMPLES: The number of prior-to-production samples for this contract is indicated below for each item. Each sample shall be printed and constructed as specified and must be of the size, kind, and quality that the contractor will furnish.

--Items 1, 3, 4, & 5: Forty (40) priors each. Each proof recipient will receive a set of ten with each set containing all ten dummy records and the appropriate mail date as specified in "SCHEDULE". Proofs must include all variable data that will print on the final product (see "DESCRIPTION").
--Item 2: Four (4) priors. Each proof recipient will receive one prior.

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

Contractor is responsible for all costs incurred in the delivery of the proofs. The Government will approve, conditionally approve, or disapprove the samples. Approval or conditional approval shall not relieve the contractor from complying with the specifications and all other terms and conditions of the contract. A conditional approval shall state any further action required by the contractor. A notice of disapproval shall state the reasons therefore.

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

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

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

Manufacture of the final product prior to approval of the samples submitted is at the contractor's risk. SAMPLE(S) WILL NOT BE RETURNED TO THE CONTRACTOR. All costs, including the costs of all samples, shall be included in the contract price for the production quantity.

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

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 WinZIP (.zip) file format.

BINDING:
- Items 1, 2, 3, 4, & 5: Trim 4 sides. Fold from 8-1/2 x 11" to 8-1/2 x 5-1/2" with address of Items 1, 3, 4, & 5 and "Frequently Asked Questions" of Item 2 facing out. Note: For Items 1 & 2, contractor has the option to collate the flat forms and fold together or fold separately (see "ASSEMBLY" for additional information).

- Item 6: See "DESCRIPTION".

ASSEMBLY OF CONTACTS:
- Contact 1: Mailing consists of one copy of the IRS Letter C1 6132 (Item 1) and one copy of FAQ Publication 5578 (Item 2), collated head to head, folded to 8-1/2 x 5-1/2" (with Item 1 on top with address facing out) and inserted into one copy of the 6 x 9" Window Envelope (Item 6). Insert letter so that only the taxpayer name, address and barcodes show through the window. NOTE: Contractor has the option to collate the flat forms and fold together or collate pre-folded forms with folded Item 1 on top of folded Item 2.

- Contact 2: Mailing consists of one copy of the IRS Letter C2 6332 (Item 3) folded to 8-1/2 x 5-1/2" (with address facing out) and inserted into one copy of the 6 x 9" Window Envelope (Item 6). Insert letter so that only the taxpayer name, address and barcodes show through the window.

- Contact 3: Mailing consists of one copy of the IRS Letter C3 6333 (Item 4) folded to 8-1/2 x 5-1/2" (with address facing out) and inserted into one copy of the 6 x 9" Window Envelope (Item 6). Insert letter so that only the taxpayer name, address and barcodes show through the window.

- Contact 4: Mailing consists of one copy of the IRS Letter C4 6334 (Item 5) folded to 8-1/2 x 5-1/2 (with address facing out) and inserted into one copy of the 6 x 9" Window Envelope (Item 6). Insert letter so that only the taxpayer name, address and barcodes show through the window.

AD HOC MAILINGS: In addition to the 4 Contacts for the Wave, there will be Ad Hoc mailings once a week. These mailings will be divided into 2 categories:
--- 1. Ad Hoc Request: Initiated when taxpayers request a web invite letter.
--- 2. Ad Hoc Postal Non-Deliverables (PND): Initiated when USPS sends a better address.

Contractor will send the Ad Hoc Mailings via First Class Mail (reimbursable postage). NOTE: POSTAGE MUST BE METERED! Stamps are NOT acceptable.

Contractor must submit postal documentation with invoice to be reimbursed for postage. In addition, contractor must email postal documentation to Traci Cobb (tcobb@gpo.gov) and Sylvia Greene (sylvia.j.greene@irs.gov) weekly after each ad hoc mailing or at the end of each month (contractor's option).

Ad Hoc: Mailing consists of one copy of the IRS Letter C1 6132 (Item 1) and one copy of FAQ Publication 5578 (Item 2), collated head to head, folded to 8-1/2 x 5-1/2" (with Item 1 on top with address facing out) and inserted into one copy of the 6 x 9" Window Envelope without indicia (Item 6). Insert letter so that only the taxpayer name, address and barcodes show through the window. NOTE: Contractor has the option to collate the flat forms and fold together or collate pre-folded forms with folded Item 1 on top of folded Item 2.

The files will be password encrypted and uploaded to the MRF's SFTP. Note: Ad hoc files do not get processed through NCOA.

One data file will be furnished each Friday after the Contact 2 mailing. Contractor is to mail merge and mail packages on the following Tuesday. Ad Hoc mailings will continue six weeks after the Contact 4 mailing. IRS may request to extend the ad hocs past the six weeks if the contractor agrees. Ad Hoc mailings will involve approximately 6,000 taxpayers over the course of the contract.

PULLING RESPONDENTS FROM MAILINGS:
Prior to the mail-out date for contacts 2, 3, & 4, the Marketing Research Firm will deliver two pull lists to the contractor. The first pull list will be delivered three days prior to the mailing and the second pull list will be delivered one day prior to the mailing. These lists will contain the respondent IDs of participants who have recently completed the online survey or who have called to refuse the survey. The contractor will need to remove the materials for these respondents before the mail-out date.

MAILING REQUIREMENTS: Contractor to mail all copies (for all contacts) according to the schedule. In addition to the scheduled contacts per wave, on a weekly basis as needed, files will be uploaded to the MRF's SFTP to mail web invite letters as requested. Contractor is to mail First Class Mail. Contractor will be reimbursed for postage cost at the end of the contract for mailings that do not use the G-48 indicia. Contractor must submit postal documentation with invoice to be reimbursed for postage.

CASS & PAVE: Contractor must pass all files (with the exception of those furnished for proof purposes and for the ad hoc mailings) against a USPS Code Accuracy Support System (CASS) certified software address hygiene program. Contractor's software must also be Presort Accuracy Validation and Evaluation (PAVE) certified.

NCOA Link Processing, LACSLink, & Delivery Point Validation (DPV): Contractor is responsible for taking the IRS raw data files (with the exception of those furnished for proof purposes and for the ad hoc mailings) and passing the files against the National Change of Address Link (NCOALINK), LACSLink, and Delivery Point Validation (DPV) file using a licensed USPS Full Service Provider.

Contractor must select the new move addresses from the mail file, verify the service center code of the new move addresses, make all necessary service center code corrections using the furnished electronic file, and merge the new move addresses back into the mail file.

In addition, any changes must be furnished by the print contractor to the Marketing Research Firm via SFTP within one week of the update. All NCOA files should be an Excel spreadsheet with the following variables:

[ID] [Name] [Previous Street 1] [NCOA Street 1] [NCOA Street 2] [NCOA City] [NCOA State] [NCOA Zip] [NCOA Zip4]

NOTE: If the file is furnished as Comma Delimited file, the contractor will need to manipulate the file in order for the "0" to print. Files saved in a comma delimited format do not allow for leading zeros in a zip code. Contractor must know how to work this file in order to print the zip code correctly.

Presort: Contractor must utilize a commercially prepared software package for assigning the mail file in an approved 5-digit format in order to maximize postage savings.

Orders which result in mailings of less than 200 pieces will require the contractor to apply the appropriate postage to each mailing. Contractor will be reimbursed for this postage by submitting a properly completed Postal Service Form 3606 Certificate of Bulk Mailing with the invoice. For reimbursable postage, the contractor must apply metered postage. Loose and/or sloppy metering tabs will not be allowed. Metering tabs must NOT extend past the edge of the envelope and should not lift off causing ragged edge when sent through USPS equipment. Stamps are NOT acceptable! NOTE: Form 13456 is not required for these mailings.

USPS Regulation Compliance: The contractor must comply with all U.S. Postal Service regulations governing the preparation of First Class rate mailings which are in effect at the time of the mailing, including the issuance of the required forms (mailing statements) and the weighing of shipments.

The current Domestic Mail Manual (DMM) has specific requirements regarding the minimum and maximum package sizes and must be adhered to by all mailers.

Mailing Rate: The Postal Service will verify the total weight of the mailing. The contractor must comply with all current Domestic Mail Manual (DMM) regulations governing use of First Class Mail.

Indicia: The Government will furnish a permit number and indicia for the First Class Mail. A PS Form 3602, Statement of Mailing with Permit Imprints must be completed and submitted to the entry post office for all mailings using permit imprint.

Internal Wrapping or Tying: All bundles containing mixed carrier routes or 3/5-digit ZIP codes require internal wrapping or tying in direct packages of ten or more letters. See current Domestic Mail Manual for details.

Postal Pallets: The USPS will provide pallets upon contractor's request, or contractor may use their own pallets that meet postal requirements, at his own expense. Loaded pallets must be wrapped with a shrinkable or stretchable plastic strong enough to retain the integrity of the pallet during transportation and handling. Pallets must be prepared in accordance with the requirements in the current Domestic Mail Manual for "Packages and Bundles Presented on Pallets" and "Palletizing Sacks". See the current DMM for preparation requirements for palletizing First-Class Mail. Packages must be palletized separately from sacks. The sack tags must be bar coded and readable by USPS equipment. Further details on pallet loading and flagging may be obtained by consulting local Postal Customer Representatives.

Pallet Staging and Storage: Loaded pallets must be assembled and stored "staged" for eventual turn over to U.S. Postal Service beginning no sooner than the date specified in the Schedule. The pallets are to be staged in an order so that the furthest destinations will be turned over first and the closest destinations last.

Upon completion of each mail contact: Contractor must submit completed Form 13456 via email to postage@publish.no.irs.gov, Sylvia.J.Greene@irs.gov, and tcobb@gpo.gov. The print contractor is required to electronically complete and submit Form 13456 to the IRS within three days of mailing. Any delay or missing input could result in delay of payment. For contractor's convenience, Form 13456 is provided as a fillable PDF file. The IRS Publishing Specialist will complete the top portion of the form prior to emailing the form to the contractor.

Contractor must read instructions furnished with F13456 which instructs the contractor on what data must be captured and the correct naming nomenclature for the PDF files. For any questions, please contact Sylvia Greene (Sylvia.J.Greene@irs.gov).

In addition, contractor must email postal documentation to Traci Cobb (tcobb@gpo.gov) and Sylvia Greene (Sylvia.J.Greene@irs.gov) weekly after each ad hoc mailing or at the end of each month (contractor's option).

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

SCHEDULE:
Purchase Order, print files, and dummy data will be emailed to the contractor on or before **March 31, 2022**.

Contractor to email soft proofs to the agency on or before **April 8, 2022.** Contractor must provide hard proofs within ten workdays of receiving soft proof approval.

For the duration of the contract, any NCOA changes must be furnished by the contractor to the Marketing Research firm via SFTP within one week of the NCOA update (see "MAILING REQUIREMENTS" for additional information).

F.O.B. DESTINATION:
- Deliver a total of 18 copies to one address on or before October 5, 2022 - see "DISTRIBUTION" section for quantity breakdown per Item and address information.

F.O.B. CONTRACTOR'S CITY: NO EARLY MAILOUT PERMITTED! See below mailing schedule:
Wave 1 Mail Dates:
- Contact 1: Contractor to mail one assembled set (see "ASSEMBLY" section for items) to approximately* 40,010 individual addresses (*per furnished distribution list) on NOT before October 14, 2022.

- Contact 2: Contractor to mail one assembled set (see "ASSEMBLY" section for items) to approximately* 40,010 individual addresses (*per furnished distribution list) on NOT before October 28, 2022.

- Contact 3: Contractor to mail one assembled set (see "ASSEMBLY" section for items) to approximately* 40,010 individual addresses (*per furnished distribution list) on NOT before November 18, 2022.

- Contact 4: Contractor to mail one assembled set (see "ASSEMBLY" section for items) to approximately* 40,010 individual addresses (*per furnished distribution list) on NOT before December 2, 2022.

Ad Hoc: Contractor to mail one assembled set (see "AD HOC MAILINGS" section for items) as requested. Ad Hoc mailings will continue through January 17, 2023. IRS may request to extend the ad hocs if the contractor agrees.

All mailings, except when otherwise indicated, must be First Class Pre-Sort. The contractor is cautioned that the "Postage and Fees Paid" indicia may be used only for the purpose of mailing material produced under this contract. All mailings must conform to US Postal Guidelines for Domestic Mail as applicable. The contractor will pay postage for mailings (as indicated) that do not mail using the G-48 indicia. Contractor will be reimbursed for only this postage cost at the end of the contract. Contractor must submit postal documentation with invoice to be reimbursed for postage.

DISTRIBUTION:
F.O.B. Destination (Hard Proofs):
- Deliver hard proofs (see below) to four different addresses. Complete addresses will be furnished after award.
Proof recipient #1: Residential address in Oakton, VA 22124.
Proof recipient #2: Residential address in Washington, DC 20002.
Proof recipient #3: Residential address in Jefferson City, MO 65109.
Proof recipient #4: Residential address in Fayetteville, GA 30214.

Each proof recipient receives the following proofs (see "PROOFS" for additional information on proof requirements).

-- 10 priors of Item 1
-- 1 prior of Item 2
-- 10 priors of Item 3
-- 10 priors of Item 4
-- 10 priors of Item 5
-- 1 content/construction proof of Item 6 with indicia
-- 1 content/construction proof of Item 6 without indicia

Note: Contractor must email tracking numbers for all hard proofs to Traci Cobb (tcobb@gpo.gov) and Sylvia Greene (Sylvia.J.Greene@irs.gov).

F.O.B. Destination (Printed Copies):
Deliver copies of each Item as indicated below to a residential address in Oakton, VA 22124. Complete address will be furnished after award.

NOTE: All merge fields if applicable should be left blank. No variable data will be supplied for these items.

-- 3 copies of Item 1 (IRS Letter (C1) 6132)
-- 3 copies of Item 2 (FAQ (C1) Pub 5578)
-- 3 copies of Item 3 (IRS Letter (C2) 6332)
-- 3 copies of Item 4 (IRS Letter (C3) 6333)
-- 3 copies of Item 5 (IRS Letter (C4) 6334)
-- 3 copies of Item 6 (6 x 9" Window Envelope without indicia)

F.O.B. Contractor's City: See "AD HOC MAILINGS" and "MAILING REQUIREMENTS".

QUALITY ASSURANCE THROUGH ATTRIBUTES: The bidder agrees that any contract resulting from bidder's offer under these specifications shall be subject to the terms and conditions of GPO Pub. 310.1 "Quality Assurance Through Attributes – Contract Terms" in effect on the date of issuance of the invitation for bid. GPO Pub 310.1 is available without charge from: U.S. Government Publishing Office, Atlanta Regional Office, 3715 Northside Parkway, NW, Suite 4-305, Atlanta, Georgia 30327.

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:

Items 1 through 5:

Attribute Specified	Specified Standard	Alternate Standard*
P-7 Type Quality and Uniformity	Approved Priors	Approved PDF (Page Integrity)

Item 6:

Attribute Specified	Specified Standard	Alternate Standard*
P-7 Type Quality and Uniformity	Approved PDF (Page Integrity)	File Setup/Average Type Dimension

*In the event that the Specified Standard is waived, the Alternate Standard will serve as its replacement.

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

OFFERS: Offers must include the cost of all materials and operations for the total quantity ordered in accordance with these specifications. In addition, a price must be submitted for additional copies (per each, per hundred, or per thousand). The price of the additional quantities must be based on a continuing run, exclusive of all basic or preliminary charges and will NOT be a factor for determination of award.

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

The Jacket number (623-849) and bid opening date (March 22, 2022) must be specified in the subject line of the emailed bid submission. Bids received after 2:00pm Eastern Time on the bid opening date specified above will not be considered for award.

NOTE: Bidders are to fill out, sign/initial, and return pages 16 and 17.

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.

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

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

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

PAYMENT: Submitting invoices for payment via the GPO fax gateway utilizing the GPO barcode coversheet program application is the most efficient method of invoicing. Instruction for using this method can be found at the following web address: http://winapps.access.gpo.gov/fms/vouchers/barcode/instructions.html.

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

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/vendors/how-to-get-paid.

CONTRACTOR: _____

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.

Bid Amount: _____

Additional rates:

- *Item 1:* _____ Per _____

- *Item 2:* _____ Per _____

- *Item 3:* _____ Per _____

- *Item 4:* _____ Per _____

- *Item 5:* _____ Per _____

- *Item 6:* _____ Per _____

_____
(Contractor's Initials)

(COMPLETE AND SUBMIT THIS PAGE WITH YOUR BID)

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).

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.

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

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 completed copy of all applicable pages that include the Jacket Number, Bid Price, Additional Rate, Discounts, Amendments, Bid Acceptance Period, and Bidder's Name and Signature, including 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)

****

(COMPLETE AND SUBMIT THIS PAGE WITH YOUR BID)

Exhibit #1 (12 pages)

CONTRACTOR'S SECURITY LETTER & PLANS: The contractor must email to sylvia.j.greene@irs.gov a detailed report of the inventory and tracking system and the security measures to be taken to secure any SBU information sent throughout the period the contractor has possession of taxpayer information.

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:
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.

Production Area -The contractor must provide a secure area(s) dedicated to the processing and storage of data for the Survey Packets (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 survey packets. (For further information, see "SAFEGUARDS REQUIREMENTS: Physical Storage Facility Requirements" specified herein).

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

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

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.

DATA SECURITY AND SAFEGUARD REQUIREMENTS

PROTECTION OF CONFIDENTIAL INFORMATION: The contractor must guarantee that they, and any subcontractors, will not reproduce, or allow reproduction of, any Sensitive but Unclassified Information (SBU), furnished by IRS, nor use or allow any person to use the SBU for any other purpose than mailing the surveys. (See IRS Pub. 1075 "Tax Information Security Guidelines for Federal, State, and Local Agencies.") A copy may be obtained either from the Internet by entering HTTPS://WWW.IRS.GOV then click on forms and pubs, or from the IRS by calling 1-800-829-3676). The Contractor shall assure 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 and civil penalties for violations of the Privacy Act and the Internal Revenue Code. The IRS will also provide the contractor with the video Protecting Federal Tax Information. This video is also available at www.tax.gov/sbv_pfti/. Publication 4465-A, IRS Disclosure Awareness Pocket Guide and Publication 4465-A (SP), Spanish Version, will also be provided.

SAFEGUARDS REQUIREMENTS:

Physical Storage Facility Requirements: Secured Perimeter -A dedicated, enclosed by slab to-slab walls constructed of approved materials and supplemented by periodic inspection. Any lesser-type partition

supplemented by UL approved electronic intrusion detection and fire detection systems. Unless there are electronic intrusion detection devices, all doors entering the space must be locked and strict key or combination control should be exercised in accordance with "Locking Systems for Secured Areas." See IRS Publications 1075 (Rev. 11- 2016), 4812 (Rev. 11-2021), and 4812-A (Rev. 9-2014) for additional security information. Janitorial services must be performed by cleared employees or during the daytime in the presence of cleared employees. Contractor must meet all physical security requirements as outlined in Publications 1075, 4812, and 4812-A. Contractor must set up a secure and exclusive network for all IRS files and related work. All files must be directly downloaded and stored onto a dedicated storage device (i.e., hard drive) for all IRS files and related work. When the dedicated storage device is not in use, the hard drive must be store in a security container*. At the completion of this contract or termination, the contractor is required to send all storage devices to the ordering agency for destruction.

***Security Container Requirements**: Metal containers that are lockable and have a resistance to penetration. The containers should have only two (2) keys. Strict control of keys is mandatory. Examples are mini safes, metal lateral key lock files, and metal pull drawer cabinets with center/off center lock bars secured by padlocks.

See below security control information:

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 contractis 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, Contractor Investigations, IRM 10.5.1 Privacy Policy, and IRM 10.8.1 - Information Technology (IT) Security, Policy and Guidance. Publication 4812 and IRM 10.5.1, 10.8.1 and 10.23.2 provide comprehensive lists of all security, privacy, information protection and disclosure controls and guidance.
4. Eligibility, Fitness and Suitability. Contractor (including subcontractor) personnel 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, and in accordance with IRM 10.23.2, and TD P 15-71. Contractor (including subcontractor) personnel must be found both eligible and suitable, and approved for staff- like access (interim or final) by IRS Personnel Security prior to starting work on the contract/order, and before being granted access to IRS information systems or SBU information.

5. General Conditions for Allowed Disclosure. Any SBU information, in any format, made available to or created by the contractor (including subcontractor) 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 prior written 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, each contractor (including subcontractor) personnel who requires staff-like access to SBU information shall complete, sign and submit to Personnel Security – through the CO (or COR, if assigned) — an approved Nondisclosure Agreement prior to being granted staff-likeaccess to SBU information under any IRS contract or order.

7. Training. All Contractor personnel assigned to this contract with staff-like access to SBU information must complete IRS-provided privacy and security awareness training, including the Privacy, Information Protection, and Disclosure training, as outlined in IR1052.224-9001 Mandatory IRS Security Training for Information Systems, Information Protection and Facilities Physical Access.

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 bound by the Records Management by Federal Agencies (44 U.S.C. Chapter 31) regarding the care and retention of federal records.

B. Definitions
"Federal record" as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved 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 as permitted 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 Liaison and Disclosure (PGLD, Incident Management) will review the PII Breach Reporting Form and alert the Records and Information Management (RIM) Program Office that a suspected records loss has occurred. The agency must report promptly to NARA in accordance with 36 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, andphysical 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 in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub- contractor) is required to abide by Government and [Agency] guidance for protecting sensitive, proprietary information, 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 deliverable that 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 it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

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

D. Flow down of requirements to subcontractors

1. The Contractor shall incorporate the substance of this language, its terms, 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 of the Government and not addressed elsewhere in the contract. If none are entered here, there are no other safeguards applicable to this contract action.]

(End of clause)

IR1052.239-9008 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)

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) Contractors will ensure that before gaining access to any sensitive but unclassified data (SBU) all employees review Privacy Awareness Training, made available by the IRS' Office of Privacy.

(d) 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.

CRIMINAL SANCTIONS: It is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a (i)(1) which is made applicable to contractors by 5 U.S.C. 552a (m)(1), provides that any officer or employee of an agency, who by virtue of his/her employment of official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $10,000.00.

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

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

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

Inspection: The contractor shall be subject at the option/discretion of the ordering agency, to periodical testing (but no less than annually) and evaluation of the effectiveness of information security controls and techniques. The assessment of information security controls may be performed by an agency independent auditor, security team or Inspector General, and shall include testing of management, operational and technical controls, as indicated by the security plan or every information system that maintain, collect, operate or use federal information on behalf of the IRS. The IRS and contractor shall document and maintain a remedial action plan, also known as a Plan of Action and Milestones (POA&M) to address any deficiencies identified during the test and evaluation. The contractor must cost-effectively reduce information security risks to an acceptable level within the scope, terms and conditions of the contract. The contractor has the responsibility of ensuring that all identified weaknesses are either corrected and/or mitigated. The Government shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, the Contracting Officer of the 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)).

SENSITIVE BUT UNCLASSIFIED SYSTEMS OR INFORMATION:

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

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

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

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

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

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

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

Exhibit #2 (8 pages)

PERSONNEL SECURITY AND ANNUAL TRAINING REQUIREMENTS: The IRS requires that the contractor's employees having a need for staff-like access to sensitive but unclassified 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 stafflike access to IRS data. The Government (including an IRS personnel security officer) will assess the risk level for each position and determine the need for individual security investigations.

- The IRS shall bear the cost of conducting a security screening for contractor employees requiring one.
- The Government will provide electronic copies of the required forms.
- Any costs for fingerprinting not conducted at an approved credentialing location will be borne by the contractor.
- Contractor personnel requiring investigation will not be allowed staff-like access to IRS data until approved by the IRS National Background Investigation Center (NBIC).

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.

To initiate the background investigation the contractor must complete the Risk Assessment Checklist (RAC) form and security documents: Form 13340, (Fair Credit Reporting Act), Optional Form 306 (Declaration for Federal Employment), and review and initial Notice 1379 (Tax Record Check Notice)). The IRS Human Capital Office, Personnel Security, Contractor Security Onboarding office may request additional forms to complete their investigation.

The below notice and consent will be provided as a separate document after award unless the Government waives the requirement to submit IR1052.209-9002.

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: _____

See below personnel security and training information:

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 following eligibility/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 background investigations.

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

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

Contract Duration:

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

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

c. For contractor (including subcontractor) personnel not requiring staff-like access to IRS facilities, IT systems, or SBU data, and only require infrequent access to IRS-owned or controlled facilities and/or equipment (e.g., a time and material maintenance contract that warrants access one or two days monthly), an IRS background investigation is not needed and will not be requested if a qualified escort, defined as an IRS employee or as a 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/or SBU data only upon notice of an interim or final staff-like approval from IRS Personnel Security, as defined in IRM 10.23.2 – *Contractor Investigations*, and is otherwise consistent with IRS security practices and related IRMs, to include, but not limited to:

- IRM 1.4.6 – Managers Security Handbook; IRM10.2.14 – Methods of 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 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 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 Security within 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 the gaining contract/order and representative duties/responsibilities to allow for an assessment of suitability based on position sensitivity/risk level designation);
- Denial of or revocation of staff-like access as determined by IRS Personnel Security;
- Separation, furlough, or release from employment;
- Anticipated extended absence of more than 45 days;
- Change of legal name;
- Change to employment eligibility;
- Change in gender or other distinction when physical attributes 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 security documents as identified by Personnel Security. The notice shall include the following minimum information:

- Name of contractor personnel;
- Nature of the change in status, assignment or standing (i.e., provide a brief non-personal, broad-based explanation);
- Affected contract/agreement/order number(s);
- Actual or anticipated date of departure or separation;
- When applicable, the name of the IRS facility or facilities this individual routinely works from or has staff-like access to when performing work under this contract/order;
- When applicable, contractor (including subcontractor) using contractor (or subcontractor)owned systems for work must ensure that their systems are updated to ensure personnel no longer have continued staff-like access to IRS work, either for systems administration or processing functions; and
- Identification of any Government Furnished Property (GFP), Government FurnishedEquipment (GFE), or Government Furnished Information (GFI) (to include Personal Identity Verification (PIV) credentials or badges – also referred to as SmartID Cards) provided to the contractor personnel and its whereabouts or status.

In the event the subject contractor (including subcontractor) is working on multiple contracts, orders, or agreements, notification shall be combined, and the cognizant COR for each affected contract or order (using the Contractor Separation Checklist (Form 14604 (Rev. 8- 2016)) shall be included in the joint notification along with Personnel Security. These documents (the RAC and security forms) are also available by email request to Personnel Security.

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

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

IR1052.224-9001 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 aresubject 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 all assigned briefings which are based on the responses provided on the Risk Assessment Checklist Form 14606. These responses pertaining to access to any IRS system, including basic LAN, email, and internet; access to any Sensitive but Unclassified (SBU) data; and access to any IRS facility. Since new contractor/subcontractor personnel will not have access to the IRS training system, the COR shall provide softcopy versions of each briefing.

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

   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 Publication4812.

   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)

Exhibit #3 (6 pages)

Conditional Access to Sensitive Information Non-disclosure Agreement

Project or contract name/number

Identify the nature of contract work or special project

printing and mailing survey components for Form 14463 (OS)

Identify type(s) of information *(e.g., documents, memoranda, reports, testimony, deliberations, maps, drawings, schematics, plans, assessments, etc.)*

pamphlets and envelopes

Advised by *(IRS or in the case of bureau sensitive information released to the Office of Inspector General (OIG) or Treasury Inspector General for Tax Administration (TIGTA), or the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) in accordance with a written arrangement related to the official audit/investigative functions of the OIG or TIGTA or SIGTARP for that particular matter)*

I, _____, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain United States Government documents or material containing sensitive information.

I understand and agree to the following terms and conditions:

1. By being granted conditional access to sensitive information, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement.
2. As used in the Agreement, sensitive information is 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 Title 5 U.S.C. 522a, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.
3. I am being granted conditional access contingent upon my execution of this Agreement for the sole purpose of printing and mailing survey components for Form 14463 (OS). This approval will permit me conditional access to certain information, pamphlets and envelopes and/or to attend meetings in which such information is discussed or otherwise made available to me.
4. I will never divulge any sensitive information that is provided to me pursuant to this Agreement to anyone unless I have been advised in writing by the . Should I desire to make use of any sensitive information, I will do so in accordance with paragraph 6 of this Agreement. I will submit to the IRS for security review, prior to any submissions for publication, any book, article, column or other written work for general publication that is based upon any knowledge I obtained during the course of my work on to ensure that no IRS sensitive information is disclosed.
5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of sensitive information not consistent with the terms of this Agreement.
6. Upon signing this non-disclosure agreement, I will be permitted access to official IRS documents containing sensitive information and understand that any copies must be protected in the same manner as the originals. Any notes taken during the course of such access must also be protected in the same manner as the originals.
7. If I violate the terms and conditions of this Agreement, I understand that the unauthorized disclosure of sensitive information could compromise IRS security.
8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to sensitive information. This may serve as a basis for my being denied conditional access to the IRS information, both classified and sensitive information in the future. If I violate the terms and conditions of this Agreement, the United States may institute a civil action for damages or any other appropriate relief. The willful disclosure of information to which I have agreed herein not to divulge may constitute a criminal offence.
9. Unless and until I am provided a written release by the IRS from this Agreement or any portions of it, all conditions and obligations contained in this Agreement apply both during my period of conditional access, which shall terminate at the conclusion of my work on , and at all times thereafter.
10. Each provision of this Agreement is severable. If a court should find any provisions of this Agreement unenforceable, all other provisions shall remain in full force and effect.
11. I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.
12. By granting me conditional access to information in this context, the United States Government does not waive any statutory or common law evidentiary privileges or protections that it may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

13. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 13526 or 13556; 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 USC 421 et seq.)(governing disclosures that could expose confidential Government agents), and the statutes that protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 128, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

14. My execution of this Agreement shall not nullify or effect in any manner any other secrecy or nondisclosure Agreement which I have executed or may execute with the United States Government except within the Department of the Treasury as noted in item 8, above.

15. I make this Agreement in good faith, without mental reservation or purpose of evasion.

Name	Signature	Date

This Agreement was accepted by the undersigned on behalf of the IRS as a prior condition on conditional access to sensitive information. Further release to any other third party requires execution of a nondisclosure agreement.

If applicable:
When information is shared with the Office of Inspector General or the Treasury Inspector General for Tax Administration or the Special Inspector General for TARP, for official audit/investigative purposes, the following statement must be added below the signature line. "This Agreement was accepted by the undersigned on behalf of the (identify bureau and (the Office of Inspector General or Treasury Inspector General for Tax Administration, Special Inspector General for TARP, as applicable) for conditional access to sensitive information. Further release and dissemination of (identify DO/bureau) sensitive information under this non-disclosure agreement must be in accordance with a written arrangement related to the official audit/investigative functions of the OIG or TIGTA or SIGTARP for that particular matter. Further release to any other third party requires execution of a nondisclosure agreement."

IRS COR or Business Unit Official signatory	Date
OIG or TIGTA or SIGTARP signatory	Date

Instructions for Form 15269, Conditional Access to Sensitive Information Non-disclosure Agreement

Individuals assigned to perform work for the Internal Revenue Service (IRS) who require access to Sensitive But Unclassified (SBU) information must sign a Non-Disclosure Agreement (NDA). This includes federal employees and contractor employees which includes, but is not limited to:

- Subcontractors
- Interns *(paid/unpaid)*
- Document Recovery Services
- Outside Experts
- Courier and Printing Services
- Delivery Services
- Consultants
- Sign Language Interpreters

The Contracting Officer's Representative (COR) or Business Unit (BU) official, in consultation with IRS Personnel Security (PS), will determine if the individual requires access to SBU information and warrants execution of an NDA as a condition thereof. The NDA must reference the nature of access to SBU information regarding the work performed for the IRS. If an NDA is required, the following will occur:

1. COR or BU official completes the fillable information pertaining to the IRS contract or special project, i.e., contract name/number, special project details, individual's name, nature of the work/project, types of information, documents, memoranda, reports, etc. available to the individual. The NDA is sent to the individual for review and signature.
2. Individual signs and dates the agreement and returns to the COR or BU official by email.
3. COR or BU official signs and dates agreement for acceptance on behalf of the IRS.
4. COR or BU official maintains a copy of the signed NDA in the official administrative/contract file. The copy of the NDA will be retained for as long as the information is deemed sensitive.
5. COR or BU official emails the original NDA to IRS PS Contractor Security Onboarding Team at: *HCO PS Contractor Security Onboarding hco.ps.contractor.security.onboarding@irs.gov. PS will maintain the original NDA in the personnel security file for a minimum of five years or for as long as the information is deemed sensitive.
6. COR or BU official may furnish a copy of the agreement to the individual, if requested.

Acceso Condicional a la Información Confidencial
Acuerdo de No Divulgación

Nombre/Número del proyecto o contrato

Identifique la naturaleza del trabajo o proyecto especial del contrato

printing and mailing survey components for Form 14463 (OS)

Identifique el tipo o tipos de información *(por ejemplo, documentos, memorandos, informes, testimonios, deliberaciones, mapas, dibujos, esquemas, planes, evaluaciones, etcétera)*

pamphlets and envelopes

Asesorado por *(el IRS o en el caso de información confidencial de la oficina divulgada a la Oficina del Inspector General (OIG, por sus siglas en inglés) o al Inspector General del Tesoro para la Administración Tributaria (TIGTA, por sus siglas en inglés), o el Inspector General Especial para el Programa de Alivio a los Activos en Problemas (SIGTARP, por sus siglas en inglés) conforme a un acuerdo por escrito relacionado con las funciones oficiales de auditoría/investigación de la OIG, o el TIGTA o el SIGTARP para ese asunto en particular)*

Yo, _____, por la presente doy mi consentimiento a los términos de este Acuerdo en consideración de que se me conceda acceso condicional a ciertos documentos o materiales del Gobierno de los Estados Unidos que contengan información confidencial.

Entiendo y acepto los siguientes términos y condiciones:

1. Al concederme acceso condicional a la información confidencial, el Gobierno de los Estados Unidos ha depositado especial confianza y seguridad en mí y estoy obligado a proteger esta información de la divulgación no autorizada, de conformidad con los términos de este Acuerdo.
2. Tal como se utiliza en el Acuerdo, la información confidencial es cualquier información cuya pérdida, uso indebido, o acceso o modificación no autorizado podría afectar negativamente el interés nacional o la realización de los programas federales, o a la privacidad a que tienen derecho las personas, conforme al Título 5 del Código de los Estados Unidos 522a, pero que no ha sido específicamente autorizado bajo los criterios establecidos por una Orden Ejecutiva o una Ley del Congreso para mantenerse en secreto en interés de la defensa nacional o la política exterior.
3. Se me concede acceso condicional supeditado a mi ejecución de este acuerdo con el único propósito de printing and mailing survey components for Form 14463 (OS). Esta aprobación me permitirá el acceso condicional a cierta información pamphlets and envelopes y/o asistir a reuniones en las que tal información es tratada o de otra manera puesta a mi disposición.
4. Nunca divulgaré ninguna información confidencial que se me proporcione de conformidad con este Acuerdo a nadie, a menos que haya sido notificado por escrito por . Si deseo utilizar cualquier información confidencial, lo haré de conformidad con el párrafo 6 de este Acuerdo. Enviaré al *IRS* para revisión de seguridad antes de cualquier presentación para publicación, cualquier libro, artículo, columna u otro trabajo escrito para la publicación general que se base en cualquier conocimiento que obtuve durante el curso de mi trabajo en para asegurar de que no se divulgue ninguna información confidencial del *IRS*.
5. Por la presente asigno al Gobierno de los Estados Unidos todas las regalías, remuneraciones y emolumentos que hayan resultado, resulten o puedan resultar de cualquier divulgación, publicación o revelación de información confidencial que no sea compatible con los términos de este Acuerdo.
6. Al firmar este acuerdo de no divulgación, se me permitirá el acceso a los documentos oficiales del IRS que contengan información confidencial y entiendo que toda copia debe ser protegida de la misma manera que el original. Toda nota tomada durante el curso de dicho acceso debe también protegerse de la misma manera que el original.
7. Si incumplo los términos y condiciones de este Acuerdo, entiendo que la divulgación no autorizada de la información confidencial podría comprometer la seguridad del *IRS*.
8. Si incumplo los términos y condiciones de este Acuerdo, dicho incumplimiento puede resultar en la cancelación de mi acceso condicional a la información confidencial. Esto puede servir como base para que en el futuro se me niegue el acceso condicional a la información del *IRS*, tanto la información clasificada como la confidencial. Si incumplo los términos y condiciones de este Acuerdo, los Estados Unidos pueden entablar una acción civil por daños o cualquier otro alivio apropiado. La divulgación intencional de la información a la que he acordado aquí no divulgar puede constituir un delito criminal.
9. A menos y hasta que el *IRS* me proporcione una liberación por escrito de este Acuerdo o de cualquier parte de este, todas las condiciones y obligaciones contenidas en este Acuerdo se aplicarán durante mi período de acceso condicional, que terminará al concluir mi trabajo en y en todo momento a partir de entonces.
10. Cada disposición de este Acuerdo es separable. Si un tribunal considera que alguna disposición de este Acuerdo no es aplicable, todas las demás disposiciones permanecerán en pleno vigor y efecto.

11. Entiendo que el Gobierno de los Estados Unidos puede buscar cualquier recurso disponible para hacer cumplir este Acuerdo, incluso, pero no limitado a, la solicitud de una orden del tribunal que prohíba la divulgación de información en el incumplimiento de este Acuerdo.

12. Al concederme acceso condicional a la información en este contexto, el Gobierno de los Estados Unidos no renuncia a ningún privilegio o protección probatorio legal o de derecho consuetudinario que pueda afirmar en cualquier procedimiento administrativo o judicial para proteger cualquier información confidencial a la que se me haya dado acceso condicional conforme a los términos de este Acuerdo.

13. Estas restricciones son consistentes con, y no sustituyen, contradicen ni de otra manera alteran las obligaciones, derechos o responsabilidades del empleado establecidos por las Órdenes Ejecutivas 13526 o 13556; la Sección 7211 del Título 5 del Código de los Estados Unidos (que rige las divulgaciones al Congreso); la Sección 1034 del Título 10 del Código de los Estados Unidos, según enmendada por la Ley de Protección de Denunciantes Militares (que rige las divulgaciones al Congreso por miembros de las Fuerzas Armadas); la Sección 2302(b)(8) del Título 5 del Código de los Estados Unidos, según enmendada por la Ley de Protección de Denunciantes (que rige las divulgaciones de ilegalidad, despilfarro, fraude, abuso o amenazas de salud o seguridad pública); la Ley de Protección de las Identidades de Inteligencia de 1982 (Sección 421 y siguientes del Título 50 del Código de los Estados Unidos) (que rige las divulgaciones que podrían exponer a los agentes gubernamentales confidenciales), y los estatutos que protegen contra la divulgación que puede comprometer la seguridad nacional, incluso las Secciones 641, 793, 794, 798 y 952 del Título 128 del Código de los Estados Unidos, y la Sección 4(b) de la Ley de Actividades Subversivas de 1950 (Sección 783 (b) del Título 50 del Código de los Estados Unidos). Las definiciones, requisitos, obligaciones, derechos, sanciones y responsabilidades establecidos por dicha Orden Ejecutiva y los estatutos enumerados, constituyen parte de este Acuerdo y controlan.

14. Mi ejecución de este Acuerdo no anulará ni afectará de ninguna manera ningún otro Acuerdo de secreto o no divulgación que haya celebrado o que pueda celebrar con el Gobierno de los Estados Unidos, excepto en el Departamento del Tesoro, como se indica en el punto 8, anterior.

15. Realizo este Acuerdo de buena fe, sin reservas mentales ni propósitos de evasión.

Nombre	Firma	Fecha

Este acuerdo es aceptado por el suscrito en nombre del *IRS*, como condición previa para el acceso condicional a la información confidencial. La divulgación posterior a cualquier otro tercero requiere la ejecución de un acuerdo de no divulgación.

Si es aplicable:
Cuando se comparta la información con la Oficina del Inspector General, o el Inspector General del Tesoro para la Administración Tributaria, o el Inspector General Especial para el *TARP*, para los propósitos oficiales de auditoría/investigación, se debe incluir la siguiente declaración debajo de la línea de la firma. "Este Acuerdo es aceptado por los suscritos en nombre de (identifique la oficina y (la Oficina del Inspector General, o el Inspector General del Tesoro para la Administración Tributaria, o el Inspector General Especial para el *TARP*, según se aplique) para el acceso condicional a la información confidencial. La divulgación y difusión adicional de la información confidencial de (identifique *DO*/oficina) según este acuerdo de no divulgación debe realizarse de conformidad con un acuerdo por escrito, relacionado con las funciones oficiales de auditoría/investigación de la *OIG* o *TIGTA* o *SIGTARP* para ese asunto en particular. La divulgación posterior a cualquier otro tercero requiere la ejecución de un acuerdo de no divulgación".

COR u oficial de la Unidad de Negocios del *IRS* firmante	Fecha
OIG o *TIGTA* o *SIGTARP* firmante	Fecha

Instrucciones para el Formulario 15269 (SP), Acceso Condicional a la Información Confidencial Acuerdo de no Divulgación

Las personas asignadas para realizar trabajos para el Servicio de Impuestos Internos (*IRS*, por sus siglas en inglés) que requieren acceso a Información Confidencial pero no Clasificada (*SBU*, por sus siglas en inglés) deben firmar un Acuerdo de no Divulgación (*NDA*, por sus siglas en inglés). Esto incluye a los empleados federales y empleados contratistas que incluyen, pero no se limita a:

- Subcontratistas
- Internos *(pagados/no pagados)*
- Servicios de recuperación de documentos
- Expertos externos
- Servicios de mensajería e impresión
- Servicios de entrega
- Consultores
- Intérpretes de lenguaje de señas

El Representante del Oficial de Contratación (*COR*, por sus siglas en inglés) o el oficial de la Unidad de Negocios (*BU*, por sus siglas en inglés), en consulta con la oficina de Seguridad del Personal (*PS*, por sus siglas en inglés) del *IRS*, determinará si la persona requiere acceso a la información *SBU* y garantiza la ejecución de un *NDA* como condición de dicho acuerdo. El *NDA* debe hacer referencia a la naturaleza del acceso a la información *SBU* en relación con el trabajo realizado para el *IRS*. Si se requiere un *NDA*, ocurrirá lo siguiente:

1. El *COR* o el oficial de la *BU* completa la información rellenable relacionada con el contrato o proyecto especial del *IRS*, es decir, el nombre/número del contrato, detalles del proyecto especial, nombre de la persona, naturaleza del trabajo/proyecto, tipos de información, documentos, memorandos, informes, etcétera, disponibles para la persona. El *NDA* se envía a la persona para su revisión y firma.
2. La persona firma y fecha el acuerdo y lo devuelve al *COR* o al oficial de la *BU* por correo electrónico.
3. El *COR* o el oficial de la *BU* firma y fecha el acuerdo para la aceptación en nombre del *IRS*.
4. El *COR* o el oficial de la *BU* guarda una copia del *NDA* firmado en el expediente oficial administrativo/del contrato. La copia del *NDA* se conservará mientras la información se considere confidencial.
5. El *COR* o el oficial de la *BU* envía por correo electrónico el *NDA* original al equipo de incorporación de seguridad de los contratistas de la oficina de *PS* del *IRS*, al: **HCO PS Contractor Security Onboarding* hco.ps.contractor.security.onboarding@irs.gov. La oficina de *PS* guardará el *NDA* original en el archivo de seguridad del personal por un mínimo de 5 años o mientras la información se considere confidencial.
6. El *COR* o el oficial de la *BU* puede proporcionar una copia del acuerdo a la persona, si se solicita.