Jacket: 523-736

Title: Publication 5474 (12-2020) Catalog Number 75188B / IRS Freefile Postcard

Agency: IRS

Bid Opening: January 25, 2021 at 2PM

Contractor Name	Bid	Terms		Discounted Total
Specialty Print Communications	$55,673.32	5.0%	21 days	$52,889.65
Cenveo Worldwide Eureka MO	$56,033.00		days	$56,033.00
Source One Graphics	$67,603.00	2.0%	30 days	$66,250.94
Advantage Mailing	$79,930.30	1.0%	20 days	$79,131.00

BID OPENING: Bids shall be opened at 2:00pm, prevailing Eastern Standard Time, on January 25, 2021 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: January 21, 2021

ANY QUESTIONS BEFORE AWARD CONCERNING THESE SPECIFICATIONS, CALL (404) 605-9160, EXT. 32704 (TRACI COBB). NO COLLECT CALLS.

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)).

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 the IRS Non-Disclosure Agreement in "EXHIBIT #3".
2. The contractor must complete and submit two 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 the IRS Non-Disclosure Agreement in "EXHIBIT #3".
2. The contractor must complete and submit two 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 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 Erika Bryant (Erika.J.Bryant@irs.gov) and Traci Cobb (tcobb@gpo.gov). The proposed Quality Systems Plans are subject to Government approval.

POST AWARD CONFERENCE: A post award conference with GPO, IRS, and the contractor's representative 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 the mailing portion of this contract.

PREDOMINANT PRODUCTION FUNCTION: The predominant production function for this procurement is the printing (including variable data) and mailing of the postcards.

PRODUCT: Postcards

FORM NO/TITLE: Publication 5474 (12-2020) Catalog Number 75188B / IRS Freefile Postcard

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

QUANTITY: 2,510,058 copies with variable data + 50 QARC's without variable data

PAGES: Face and Back

TRIM SIZE: 6 x 4-1/4" (No variation in trim size allowed!)

DESCRIPTION:
Face prints full color matter via 4-color process with uncommon bleed on the left and right margins. Back prints full color matter via 4-color process with no bleeds. Prints head to head. Variable data information prints in Black ink on the back of all copies except for the QARC's. Contractor's option to flood gloss aqueous coat the face and gloss aqueous coat the left half of back (as to not interfere with the address area on the back).

The proofs and 10 agency samples will be imaged with the following variable data:

0000000000********ECRLOT******C-001
RESIDENT
3651 S. Interregional Hwy, MS 1450
Austin, TX 78741-7855
(Apply Delivery Point Barcode here in IMb format.)

NOTE: Postcards must be printed via OFFSET printing on a minimum 4-color press with one single pass. Digital printing, direct imaging (toner), and inkjet* printing are not acceptable for the postcard. *Inkjet printing is acceptable for the variable data only.

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

- The contractor will be provided a zipped and secure Microsoft Excel spreadsheet that will contain the taxpayer addresses on multiple tabs. The spreadsheet will be furnished via email or uploaded to the contractor's SFTP a minimum of five workdays prior to the mail date. Agency will verbally provide password to the contractor after award. Contractor's SFTP must meet the National Institute of Standards and Technology (NIST) SP 800 security guidelines.

- IRS Form 13456 (IRS Publishing Postage Report) in a fillable PDF file will be furnished by IRS after award via e-mail ***.

*** Contractor is required to have Internet access, provided through their Internet Service Provider (ISP) with email and a web browser equivalent to Internet Explorer 6.0 or Netscape 4.0. The contractor is also required to have Adobe Acrobat 7.0 (or more recent) software (not Adobe Reader) and the capability to receive via email and open file attachments compressed into a SecureZip (.zip) file format.

ELECTRONIC MEDIA:
- PLATFORM: Unknown
- SOFTWARE: ADDITIONAL SYSTEM TIME IS REQUIRED. One PDF file will be provided. NOTES: 1) File is setup with a trim size of 7 x 5". Contractor to create page layout, including proportionately reducing image as necessary, to image as specified (trim size, bleed margins, ink colors). 2) Contractor to create variable data fields.
- COLOR: Identified as CMYK and 6 Pantone/Spot colors. Contractor to convert Pantone/Spot colors to CMYK.
- FONTS: All fonts are Embedded and/or Embedded Subset.
- OUTPUT: 175-line screen.

NOTE: GPO Imprint does NOT print on this order.

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., except 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 deliverable) 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, PostScript files, Adobe Acrobat Portable Document Format (PDF) files, or 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.

JCP Code L12, White No. 2 Gloss-Coated Cover, Basis Size 20 X 26", Basis Weight 80#

INK: If lithographic ink is used in the performance of this contract, the ink shall contain not less than the following percentages of vegetable oil: (a) news ink, 40 percent; (b) sheet-fed and forms ink, 20 percent; and (c) heat-set ink, 10 percent. High quality color process printing on high-speed heat-set presses is excepted when slow drying time significantly increases production costs.

4-color process + gloss aqueous coat (contractor's option - see "DESCRIPTION" for additional information)

MARGINS: Follow file setup* - uncommon bleed on the right and left margins of the face; adequate gripper on the balance. *See “ELECTRONIC MEDIA” for additional information.

PROOFS: Deliver the following proofs (*) to the department on or before February 3, 2021. Contractor must email proof tracking numbers to Erika Bryant (Erika.J.Bryant@irs.gov) and Traci Cobb (tcobb@gpo.gov) on day of shipping.

Contractor is responsible for all costs incurred in the delivery of proofs. All proofs will be withheld not longer than 1 workday from date of receipt by the Government** to date of proof approval/disapproval via email. **NOTE: The date of receipt by the Government is NOT considered the first workday.

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". After receiving an approval to print, contractor is responsible for maintaining proper output and complying with all USPS requirements for printed product.

NOTE: Proofs must contain the variable data as indicated under "DESCRIPTION". Proof approval is not for the optional endorsement line, delivery point code, and IMb. The contractor is responsible for ensuring the accuracy,

readability, and placement of the optional endorsement line, delivery point code, and IMb. These elements must meet USPS requirements at the time of mailing.

(*) CONTENT PROOF: Three*** complete digital color CONTENT proofs 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, and trimmed to the finished size/format of the product.

(*) INKJET PROOFS: Three*** INKJET proofs that are G7 profiled and use pigment-based inks. A proofing RIP that provides an option for high quality color matching (such as Device Links Technology and/or ICC Profiles Technology), and meets or exceeds industry tolerance to ISO 12647-7 Standard for Graphic Technology (as of 3/19/09, and future amendments) must be utilized plus GRACoL 2006 Coated #1 specifications (CGATS TR006) must be achieved. Output must be a minimum of 720 x 720 dpi on a GRACoL or SWOP certified proofing media. Proofs must contain the following color control strip to be evaluated for accuracy: IDEAlliance ISO 12647-7 Control Strip 2009 or 2013(i1).

Proofs must contain color control bars (such as Brunner, GATF, GRETAG, or RIT) for each color of ink on the sheet. Control bars must be placed parallel to the press's ink rollers and must show areas consisting of minimum 1/8 x 1/8 solid color patches; tint patches of 25, 50 and 75%; dot gain scale; and gray balance patches for process color (if applicable). These areas must be repeated consecutively across the sheet. The make and model number of the proofing system utilized shall be furnished with the proofs.

These proofs must contain all elements, be in press configuration, and indicate margins. Proofs will be used for color match on press. Direct to plate must be used to produce the final product with a minimum of 2400 x 2400 dpi.

***Contractor is to make three sets of proofs - send two sets to the agency (see "DISTRIBUTION" for addresses) and keep one set at the contractor's plant. The agency will email approval and/or corrections to the contractor. Proofs will not be returned to the contractor.

IT IS UNDERSTOOD THAT THE PROOFS SUPPLIED UNDER THIS CONTRACT WILL MATCH THE FINAL OUTPUT.

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.

BINDING: Trim 4 sides.

MAILING REQUIREMENTS: Contractor is to mail using the IRS Presort Standard Postage and Fees Paid G-48 indicia. 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 be required to follow all standards/requirements for converting addresses for USPS Presorted Standard Rate postage discounts. Prior to mailing, the contractor must run mailing addresses through commercial address cleansing and sortation programs in order to meet all USPS requirements for maximum discounts at time of mailing.

CASS & PAVE: Contractor must pass the data file 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 file and passing the file against the National Change of Address Link (NCOALINK), LACSLink, and Delivery Point Validation (DPV) file using a licensed USPS Full Service Provider.

The contractor must email Erika Bryant (Erika.J.Bryant@irs.gov) and Traci Cobb (tcobb@gpo.gov) the total mail quantity after the file is processed through NCOA. Any leftover shells due to the difference in the print quantity and the quantity after NCOA must be destroyed beyond recognition upon completion of the contract.

Variable Imaging: Contractor will be responsible for imaging the variable mailing address on back of postcard. The variable address imaging may be accomplished by either impact printers or non-impact printers. Adhesive labels are not an option for any variable data imaging.

Address imaging content/location must meet all USPS requirements for all Presorted Standard Rate discounts at time of mailing. NOTE: Contractor must ensure that the font size used for the address/IMb block does not interfere with IMb clearance requirements. IMb must be readable for post office processing and all elements accurate and properly placed on mail piece.

Address Recipient Notice: Contractor is to address recipient at all addresses as "RESIDENT". Addressing is not to contain any individual resident name(s).

The contractor must format mailing addresses to image the carrier route endorsement on the optional endorsement line (OEL) and "RESIDENT", address, city, state, and zip code plus. The contractor will be required to take information from the file and format it to create an 11-digit Delivery Point Code in the Intelligent Mail Barcode format. The routing code must contain a delivery point code from CASS-certified software that accurately matches the delivery address.

The Delivery Point code is to be imaged in accordance with the USPS Domestic Mail Manual at time of mailing. It must be on all 3/5 digit and basic mail, and may print on carrier route mail.

Optional: For the Mailer Identifier field contained in the IMb, the contractor may use the IRS number: 901035873 to identify ownership. IRS number is to be used only for the mailing produced under this contract.

Variable Imaging for 10 agency samples: See "DESCRIPTION".

USPS Regulations: The contractor must comply with all USPS regulations governing the preparation and use of the Presorted Standard Rate at the time of mailing, including the issuance of the required forms (mailing statements) and the weighing of shipments.

Indicia: The contractor will need to comply with all DMM requirements for use of Presorted Standard Mail indicia and must check to verify that IRS' G-48 permit is on file with the drop-off post office location. If IRS G-48 indicia is not on file at receiving postal facility, the contractor MUST notify Erika Bryant (Erika.J.Bryant@irs.gov) and Traci Cobb (tcobb@gpo.gov) to arrange to have the filing completed in time to meet mail date.

Mailing Location: Contractor must email Erika Bryant (Erika.J.Bryant@irs.gov) and Traci Cobb (tcobb@gpo.gov) with the location (post office, city, state) from which any required mailing will be made.

Contractor’s Required Documentation (Postage Statements): The contractor must complete and submit via email a portable document file (PDF) to the IRS within three workdays after the final turnover of mail packages. For contractor's convenience, Form 13456 "IRS Publishing Postage Report" is provided as a fillable PDF file. Contractor must follow the instructions of how to fill in the data fields of the dates, rename the PDF file, and email the PDF as detailed on Page 2 of Form 13456. The PDF should be sent in a single email and the total file size of the e-mail must be 10 MB or less. If the size exceeds 10 MB, then multiple emails must be used. E-mail the PDF to postage@publish.no.irs.gov, Erika Bryant (Erika.J.Bryant@irs.gov), and Traci Cobb (tcobb@gpo.gov). The IRS will complete the fields, in the "IRS Use Only" section of the form prior to e-mailing the form to the contractor. If there is any information missing or incorrect, please contact Erika Bryant (470-769-2030).

The PDF to be submitted to the IRS should be the Form 13456 and all related postal paperwork that has been combined into a single PDF. No scanned copy of the Form 13456 is allowed. Please fill out the provided PDF file

for Form 13456, add the postal paperwork (which can be scanned) to the PDF file, save it and submit it to IRS by email.

The contractor must complete Form 13456 per the supplied instructions on the form and fill in the following fields: name of contractor, contact person at contractor, telephone number of contact person, e-mail of contact person, mailing start date, mailing end date.

The contractor is responsible for capturing six data elements from every postage statement type (i.e. USPS Form 3600-EZ, 3600-PM, 3600-R, 3602-G, 3602-R, 3605-BPR, 3605-PP, 3607-R, 3608-R, 3651-M or 3660-R). The six elements are: (1) post office zip code, (2) postage statement date, (3) total pieces mailed, (4) copies mailed (5) postage amount, and (6) postage statement type. The form must contain only postage information for the designated IRS requisition number.

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

Prior to emailing the combined PDF file, the contractor must rename the file. The file should be named using 9 digits of the Requisition Number, Post Office Zip Code, (first) Mailing Date, (last) Mailing Statement Date and .pdf (see below). In the event that both mailing statement dates are the same, the first and last dates in the file name can also be the same.

Examples: For requisition number 2020-12345, the file name will be: 2020-12345_16625_01-02-10_01-15-10.pdf. If the file size is too large to email, the contractor will have to create multiple PDF files and add a suffix to the file name starting with the letter "a" then "b", etc. (i.e. 2020-12345_16625_01-02-10_01-15-10a.pdf).

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

Contractor must not combine postage associated to multiple print order/requisition numbers in a single email transmission.

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

PACKING: Agency samples - pack suitable per shipping container.

NOTE: All shipping cartons require a carton label. Noncompliance with the labeling and marking specifications on this order may be cause for the Government to reject the shipment at destination and return it to the contractor at his/her expense. The Government may, at its option, relabel and/or remark in accordance with the specifications and charge all costs to the contractor. There will be a minimum charge of $50.00 per order (per Jacket) for all labeling and marking corrections that are made by the Government due to the contractor's failure to label/mark all cartons per specifications and Contract Terms.

SCHEDULE:
Purchase Order and print file will be emailed to the contractor on or before **January 29, 2021**.

Deliver proofs on or before **February 3, 2021**.

Data file will be provided to the contractor on or before **February 11, 2021**.

F.O.B. Contractor's City – Mail Copies:
- Mail a total of approximately 2,510,048 individual postcards* on or before **February 18, 2021**. NOTE: Form 13456, Contractor's Postage Reporting Documentation (including all PS Form 3602s), due to IRS to verify mailings

on or before **February 23, 2021**. *Exact mail quantity will be determined after the data file is processed through NCOA.

F.O.B. Contractor's City – Agency Copies:
- Ship a total of 10 copies to two addresses on or before **February 18, 2021**- see "DISTRIBUTION" section for complete addresses and quantity breakdowns. NOTE: These copies will have the "IRS Austin, TX address" - see "DESCRIPTION" section for address to image onto samples.

Copies must be shipped GROUND via a furnished IRS Small Package Carrier (UPS) account number. Contractor must notify the GPO contract administrator if the contractor does not have such an account, and one will be established for that contractor. The contractor cannot be reimbursed for using his or her own small package carrier account.

Contractor must email tracking numbers to Erika Bryant (Erika.J.Bryant@irs.gov) and Traci Cobb (tcobb@gpo.gov) no later than one business day after shipping. Include GPO Jacket Number & IRS Requisition Number in the subject line of the email.

DISTRIBUTION:
F.O.B Destination:
- Deliver one set of proofs to residential address: Erika Bryant (470-769-2030), 1573 Mathews Manor Drive, Jacksonville, FL 32211.

- Deliver one set of proofs to residential address: Juan Goldstrom (240-613-6214), 6101 Cheverly Circle, Cheverly, MD 20785.

NOTE: Contractor must e-mail tracking number for the proof shipments to Traci Cobb (tcobb@gpo.gov) and Erika Bryant (Erika.J.Bryant@irs.gov) as soon as available.

F.O.B. Contractor's City – Mail Copies:
- Mail a total of approximately 2,510,048 individual postcards*. *Exact mail quantity will be determined after the data file is processed through NCOA.

F.O.B. Contractor's City – Agency Copies:
- Ship 5 imaged samples (see "DESCRIPTION" for address to image) to residential address: Erika Bryant (470-769-2030), 1573 Mathews Manor Drive, Jacksonville, FL 32211.

- Ship 5 imaged samples (see "DESCRIPTION" for address to image) to residential address: Juan Goldstrom (240-613-6214), 6101 Cheverly Circle, Cheverly, MD 20785.

QUALITY ASSURANCE RANDOM COPIES: The contractor is required to submit 50 quality assurance random copies without variable data to test for compliance against specifications. The contractor must divide the entire order into equal sublots and choose a copy from a different general area of each sublot. The contractor will be required to certify that copies were selected as directed using GPO Form 917-Certificate of Selection of Random Copies (located on GPO.gov). Copies will be paid for at the running rate offered in the contractor's bid and their cost will not be a consideration for award. A copy of the purchase order/specifications must be included.

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

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 II
(b) Finishing (item related) Attributes – Level II

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

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

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

Attribute Specified	Specified Standard	Alternate Standard*
P-7 Type Quality and Uniformity	Approved Proofs	File Setup
P-10 Process Color Match	Approved Proofs	File Setup

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

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 (523-736) and bid opening date (January 25, 2021) must be specified in the subject line of the emailed bid submission. Bids received after 2:00pm EST on the bid opening date specified above will not be considered for award.

NOTE: Bidders are to fill out, sign/initial, and return pages 11 and 12.

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 rate: _____ 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: _____ Date: _____ Contracting Officer: _____ Date:_____
(Initials) (Initials)

****
****

_____
(Contractor's Initials)

(COMPLETE AND SUBMIT THIS PAGE WITH YOUR BID)

Exhibit #1 (11 pages)

CONTRACTOR'S SECURITY LETTER & PLANS: The contractor must email to Erika Bryant (Erika.J.Bryant@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:
(a) Materials – How all accountable materials will be handled throughout all phases of production. This plan shall also include the method of disposal of all production waste materials.

(b) Production Area – The contractor must provide a secure area(s) dedicated to the processing and storage of data for the 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 subcontractor's, 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 HTTP://WWW.IRS.GOV then click on forms and pubs, or from 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, 4812, and 4812-A, 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 stored 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 BUT UNCLASSIFIED INFORMATION (MAY 2018)

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

- Returns and Return Information
- Sensitive Law Enforcement Information
- Employee Information
- Personally Identifiable Information
- Other Protected Information

2. Confidentiality requirements for tax returns and return information 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).

3. Contractors who perform work at contractor (including subcontractor) managed sites using contractor or subcontractor managed IT resources shall adhere to the general guidance and specific security control standards or requirements contained in Publication 4812, Contractor Security Controls, IRM 10.23.2 - Personnel Security, Contractor Investigations and IRM 10.8.1 - Information Technology (IT) Security, Policy and Guidance. Typically, all contracts that require contractor (including subcontractor) employees to handle, manage, or process SBU information shall be protected at the moderate risk level. Publication 4812 and IRM 10.8.1 and 10.23.2 provide comprehensive lists of all security controls and guidance.

4. Eligibility, Fitness and Suitability. Contractor (including subcontractor) personnel hired for work within the United States or its territories and possessions and who require 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 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) employees must be favorably adjudicated prior to starting work on the contract/order or before being granted staff-like access (or interim staff-like access, if approved by Personnel Security) to IRS information systems or SBU information.

5. General Conditions for Allowed Disclosure. Any SBU information, in any format, made available to contractor (including subcontract) 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 a duly authorized officer or employee 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 10.23.2.17 - Nondisclosure Agreement for Sensitive but Unclassified Information, each contractor (including subcontractor) employee who requires 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 access to SBU information under any IRS contract or order.

7. 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.

8. Incident and Situation Reporting. Contractors and subcontractors are required to report a suspected or confirmed breach in any medium or form, including paper, oral, and electronic, as soon as possible and without unreasonable delay. All incidents related to IRS processing, information or information systems shall be reported within one (1) hour to the CO (GPO, Traci Cobb at tcobb@gpo.gov) and COR (Erika Bryant (Erika.J.Bryant@irs.gov).

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

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

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

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

- When it has served its useful, contractual purpose, and is no longer needed to meet the contractor's (including subcontractor) other, continuing contractual obligations to the IRS or
- When the contract expires, or is terminated by the IRS (for convenience, default, or cause).

The contractor (including subcontractor) shall completely purge from its systems and Electronic Information Technology, and/or return all SBU/PII 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/PII 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 data and material, removable media (disks, CDs, thumb drives)) collected by, or provided to, the contractor been purged, destroyed or returned.

11. Subcontractors. Subcontractors of the contractor are held to the same provisions, investigative requirements, and standards of conduct for handling and protecting SBU information as employees of the prime contractor.

IR1052.239-9008 INFORMATION SYSTEMS AND INFORMATION SECURITY CONTROLS FOR CONTRACTING ACTIONS SUBJECT TO INTERNAL REVENUE MANUAL (IRM) 10.8.1 (MAY 2018)

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

(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 controls, requirements, and objectives described in applicable security control guidelines, and their respective contracts.

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

(c) Based on Title III of the E-Government Act of 2002 (Public Law 107-347), also known as the Federal Information Security Management Act of 2002 (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 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 of information and information systems in accordance with the terms and conditions of the contract and all applicable security controls. If required by the Contracting Officer's Representative, the contractor will be required to input data into a system, to be defined by the IRS, to describe the security controls being used to protect information.

(e) Flow down of clauses. The contractor shall include and flow down, in its subcontracts (or arrangements or outsourced service agreements) that entail access to SBU information by a subcontractor or agent, at any tier, the substantially 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.

IR1052.239-9009 INFORMATION SYSTEMS AND INFORMATION SECURITY CONTROLS FOR CONTRACTING ACTIONS SUBJECT TO IRS PUBLICATION 4812 (MAY 2018)

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

(a) General. 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 controls, requirements, and objectives described in applicable security control guidelines, and their respective contracts.

(b) The contractor will be required to input data into a system, to be defined by the IRS, to describe the security controls being used to protect information. Publication (PUB) 4812 Applicability. This contracting action is subject to Publication 4812 – Contractor Security Controls. PUB 4812 is available at: https://www.irs.gov/about- irs/procurement/publication-4812-contractor-security-controls

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

Flowing down from Title III of the E-Government Act of 2002 (Public Law 107- 347), also known as the Federal Information Security Management Act of 2002 (FISMA), and standards and guidelines developed by the National Institute of Standards and Technology (NIST), PUB 4812 identifies basic technical, operational, and management (TOM) security controls and standards required of under contracts for services in which contractor (or subcontractor) employees will either—

- Have 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
- Have 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.

Unless the manual specifies otherwise, the IRS-specific requirements in PUB 4812 meet the standard for NIST Special Publication (SP) 800-53 – Federal Information Systems and Organizations (Revision 3 (AUG 2009)) (*Errata as of May 1, 2010*), and the security controls, requirements, and standards described therein are to be used in lieu of the common, at-large security control standards enumerated in NIST SP 800-53 (Rev. 3).

PUB 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 controls applicable to any given contracting action subject to PUB 4812. Upon completion of any IT Cybersecurity review, the contractor must submit a plan within fifteen (15) work days after notification of the results of the review to the CO, with a copy to the COR and IT Cybersecurity, that addresses the correction and mitigation of all identified weaknesses, to include a timeline for completion.

(c) Contractor Security Representative. The contractor shall assign and identify, upon award, a Contractor Security Representative (CSR) and alternate CSR to all contracts requiring 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 controls.

(d) 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 substantially same 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.

IR1052.239-9010 – INFORMATION SYSTEM AND INFORMATION SECURITY CONTROL STANDARDS AND GUIDELINES APPLICABILITY (MAY 2018)

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

o Internal Revenue Manual (IRM) 10.8.1 – Information Technology (IT) Security, Policy and Guidance, and
o Publication 4812 – Contractor Security Controls dated 12/2017.

While IRM 10.8.1 and PUB 4812 are both based on NIST SP 800-53 (Rev. 4), 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 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 ☐ PUB 4812 only ☐ Both IRM 10.8.1 and PUB 4812

Unless the Contracting Officer (CO) determines, in consultation with Cybersecurity, that a different (or a second) security control standard or guideline is warranted, the security level selected/applied for by the

contractor under IR1052.239-9016 shall stand. In the event the Government 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 PUB 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):

- Core (C) Security Controls (Abbreviated "C")
- Core (C) plus value greater than Simplified Acquisition Threshold (SAT) (Abbreviated "CSAT")
- Core (C) plus Networked Information Technology Infrastructure (NET) (Abbreviated "CNET")
- Core (C) plus Software Application Development/Maintenance (SOFT) (Abbreviated "CSOFT")

(See PUB 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 the CO.)

b. The contractor, by signing its offer, hereby asserts to the best of its knowledge and belief that the security control level under PUB 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):

☐C ☐CSAT ☐CNET ☐ CSOFT

c. Unless the CO determines, in consultation with Cybersecurity, that a different (higher or lower) security control level is warranted for contracts subject to PUB 4812, the security level selected/applied for by the contractor will govern throughout the life of the contract. In the event the Government 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 (and for the PUB 4812 portion, use of the most stringent security control level (CSOFT)) until and unless the CO, in consultation with IT Cybersecurity, determines otherwise.

e. If required by the Contracting Officer's Representative (COR), the contractor will be required to input data into a system, to be defined by the IRS, to describe the security controls being used to protect information.

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 Washington GPO Office, may require specific measures in cases where the contractor is found to be noncompliant with contract safeguards.

BREACH RELATED TERMINATION OF DATA TRANSMISSION:

If the Government determines that an authorized recipient has failed to maintain adequate safeguards (in the transmission, retention, and/or use of SBU) or has made any unauthorized inspections or disclosures of SBU, the Government may terminate or suspend transmission of SBU to any authorized recipient until the Government is satisfied that adequate steps have been taken to ensure adequate safeguards or prevent additional unauthorized inspections or disclosures (see 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 Erika Bryant (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 (9 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 staff-like 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 ((Rev. 3-2008) (Tax Record Check Notice)). The IRS Contractor Lifecycle Management (CLM) office may request additional forms to complete their investigation.

In addition to the forms listed above, the contractor must complete the below notice and consent that will be provided as a separate document after award.

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 (MAY 2018)

As described in Department of the Treasury Security Manual (TD P 15-71), Chapter I, Section 1, Position Sensitivity and Risk Designation, Contractor personnel assigned to perform work under an IRS contract/order/agreement must undergo security investigative processing appropriate to the position sensitivity and risk level designation associated to determine whether the Contractor (including subcontractor) personnel should be permitted to work in the identified position. The Contracting Officer's Representative (COR) (in the absence of the COR, the Contracting Officer (CO)) shall work with the contractor to ensure that contractor (or subcontractor) employee is granted staff- like access to Sensitive but Unclassified (SBU) information, IRS/contractor (including subcontractor) facilities, information system/asset that process/store SBU information without the required investigation.

For security requirements at contractor facilities using contractor-managed resources, please reference Publication 4812, Contractor Security Controls. The contractor shall grant staff-like 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.

a. Contractor (including subcontractor) personnel performing under an agreement that authorizes staff-like access to and in IRS/contractor (including subcontractor) facilities, and access to SBU information or information systems are subject to (and must receive a favorable adjudication or affirmative results with respect to) the following eligibility/suitability pre-screening criteria, as applicable:

(1) IRS account history for tax compliance (for initial eligibility, as well as periodic checks for continued compliance while actively working on IRS contracts);
(2) Selective Service registration compliance;
(3) U.S. citizenship/lawful permanent residency compliance;
(4) Background investigation forms;
(5) Credit history;
(6) Federal Bureau of Investigation fingerprint results; and
(7) Prior federal government background investigations.

In this regard, Contractor shall furnish the following electronic documents to the Contractor Security Management (CSM) at CSM@irs.gov within 10 business days (or shorter period) of assigning (or reassigning) an employee to this contract/order/agreement and prior to the contractor (including

subcontractor) employee 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) Form 14606;
- Non-Disclosure Agreement (if contract terms grant SBU access); and,
- Any additional required security forms, which will be made available through CSM and the COR.

b. Tax Compliance, Credit Checks and Fingerprinting:

1. Contractors (including subcontractors) whose duration of employment exceeds 180 days must meet the eligibility/suitability requirements for 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.

2. If the duration of employment is less than 180 days or access is infrequent (i.e. 2 -3 days per month), and the contractor requires unescorted access, the contractor (including subcontractor) employee must meet the eligibility requirements for access in IRM 10.23.2.9, as well as a FBI Fingerprint result screening.

3. For contractor (including subcontractor) employees not requiring access to IT systems, a background investigation is not needed and will not be requested if a qualified escort, defined as an IRS employee or as a contractor who has been granted staff-like access, escorts a contractor meeting the conditions of number b.2 above at all times while the escorted contractor accesses IRS facilities and equipment.

The contractor (including subcontractor) employee will be permitted to perform under the contract/order/ agreement and have access to IRS facilities only upon notice of an interim or final approval, as defined in IRM 10.23.2 – Contractor Investigations, and is otherwise consistent with IRS security practices and related IRMs, to include, but not limited to, IRM 1.4.6 – Managers Security Handbook, IRM10.2.14 – Methods of Providing Protection, and IRM 10.8.1 - Policy and Guidance.

The Associate Director, Personnel Security prior to completion of the full investigation, will grant interim staff-like access approval as follows:

a. Individuals who possess a current active U.S. Government security clearance for access to classified information may be granted interim staff-like access for positions after 1) the clearance is verified through the Joint Personnel Adjudication System (JPAS), and 2) after favorable adjudication of pre-screening eligibility/ suitability checks. Individuals with Top Secret clearance may be granted interim staff-like access approval to occupy positions designated at any risk level. Individuals with Secret or Confidential clearances may be granted interim staff-like access approval to occupy positions designated Moderate or Low Risk.

b. Individuals not possessing a current or active U.S. Government security clearance for access to classified information or not possessing a prior Government personnel security investigation that meets the scope and criteria required for their position may be granted interim staff-like access approval upon receipt of all required contractor security forms, and favorable adjudication of pre- screening eligibility/suitability checks.

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.

IR1052.204-9001 NOTIFICATION OF CHANGE IN CONTRACTOR PERSONNEL EMPLOYMENT STATUS, ASSIGNMENT, OR STANDING (MAY 2018)

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

- Receipt of the employee's notice of intent to separate from employment or discontinue work under this contract/order;
- Knowledge of the employee's voluntary separation from employment or performance on this contract/order (if no prior notice was given);
- Transfer or reassignment of the employee 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 Access (RAC) as determined by the IRS
- Separation, furlough or release from employment;
- Anticipated extended absence of more than 45 days;
- Change of legal name;
- Change to citizenship or lawful permanent resident status, or employment eligibility;
- Change in gender or other distinction when physical attributes figure prominently in the biography of an individual;
- Actual or perceived conflict of interest in continued performance under this contract/order (provide explanation); or
- Death.

When required by the COR, the contractor may be required to provide the information required by this clause to the IRS using the RAC or security documents as identified by CSM.

The notice shall include the following minimum information:

- Name of contractor employee;
- 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 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 employees no longer have continued access to IRS work, either for systems administration or processing functions; and
- Identification of any Government Furnished Property (GFP), Government Furnished Equipment (GFE), or Government Furnished Information (GFI) (to include Personal Identity Verification (PIV) credentials or badges) provided to the contractor employee and its whereabouts or status.

In the event the subject contractor (including subcontractor) employee 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. 4-2015)) shall be included in the joint notification along with the CSM. These documents (the RAC and security forms) are also available by email request to CSM.

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

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

IR1052.204-9002 IRS SPECIALIZED INFORMATION TECHNOLOGY (IT) SECURITY TRAINING (ROLE-BASED) REQUIREMENTS (MAY 2018)

a) Consistent with the E-Government Act of 2002, Title III, Federal Information Security Management Act of 2002 (FISMA), Public Law 107-347, specialized information technology (IT)security training (role-based) shall be completed annually by contractor and subcontractor employees who have a significant IT security role or responsibility.

b) Identifying Candidates with a Significant Role or Responsibility for Information/IT Security. (Special Note: No contractor or subcontractor employee requiring access to a facility, information system or asset whether owned by the IRS or contractor/subcontractor that process or store IRSSBU information will be granted access without receiving interim or final access approval from personnel security prior to being able to perform under an IRS contract, order or agreement. Escort procedures shall not be utilized if contractor or subcontractor employees require access to facilities, information systems or assets that process or store IRS SBU information without first receiving a waiver from personnel security.)

(1) Internal Revenue Manual 10.8.1.4.2.2 requires prospective contractor employees to complete specialized role-based training prior to beginning duties related to their specialized IT security role(s) under the contract, order or agreement.

(2) Within 10 calendar days of contract award, establishment of an agreement, or order issuance, the Contractor shall submit to the Contracting Officer's Representative (COR) a list of contractor (including subcontractor) employees who will have a significant role or responsibility for information/IT security in the performance of the contract, will identify the specific IT security role the employee will perform under the contract, order, agreement, and will indicate whether such employee(s) has/have completed role-based training, as well as the source and title/subject of the training.

(3) In collaboration with the Enterprise FISMA Services (EFS) Group in IT Cybersecurity, Security Risk Management, and Facilities Management and Security Services (FMSS), and Contractor Security Management (CSM), the COR will review the list and confirm that the employee(s) will serve in roles that entail significant responsibility for information/IT security and will determine that the received training is adequate. The COR will inform the Contractor of the determinations. Indicators of who should complete specialized role-based training annually include but are not limited to—

• Percentage of duties devoted to information/IT security. Typically, those with 50%of their work related to FISMA duties.

• Characteristics. Those privileged network user accounts that allow individual full system permissions to the resources within their authority or to delegate that authority.

• Catalog of Roles. Those serving in roles identified in the "Required Training Hours for IRS Roles" document maintained at the IT, Cybersecurity, Security Risk Management intranet site for Specialized IT Security Training.

(c) Modified Contracts: When existing contracts are modified to include this clause and it is determined that Contractor employees performing IT Security roles and responsibilities and have not been provided the training, the Contractor will be required to provide training to the employee(s) to be completed within 45 calendar days of the determination.

(d) New/Replacement Employees: The Contractor will provide role-based training to new or replaced employees who will have a significant IT security role or responsibility under the contract prior to performance under the contract and will adhere to all other requirements set forth within this clause.

(e) Annual Requirements: Thereafter, on an annual basis within a FISMA calendar year cycle beginning July 1st of each year, a contractor employee 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 and report the training to the COR.

(f) Training Certificate/Notice: The contractor shall submit confirmation of annually completed specialized IT security training (role-based) using the Government system identified by FMSS, Identity, Credential and Access Management (ICAM), CSM for each employee identified, with a copy to the Contracting Officer and COR, upon completion of the training.

(g) Administrative Remedies: A contractor who fails to provide specialized IT security training (role-based) requirements, within the timeframe specified, may lose its access privileges.

IR1052.224-9001 MANDATORY IRS INFORMATION PROTECTION AND SECURITY AWARENESS TRAINING REQUIREMENTS (MAY 2018)

The Federal Information Security Management Act of 2002 (FISMA) requires each federal agency to provide periodic information security awareness training to all employees (including contractor and subcontractor) involved in the management, use, or operation of Federal information and information systems. In addition, contractors (including subcontractor) and their employees are subject to the Taxpayer Browsing Protection Act of 1997, which prohibits willful unauthorized inspection of returns and return information. Violation of the Act could result in civil and criminal penalties.

(a) The contractor must ensure all contractor (including subcontractor) personnel complete one or more Information Protection briefings on computer security, disclosure, privacy, physical security, and/or unauthorized access to taxpayer accounts (UNAX), as specified by Contractor Security Management (CSM). CSM can be reached at awss.csm.training@irs.gov. Individually and collectively, these briefings make up the IRS Security Awareness Training (SAT) requirements for the Service's information assets. 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 SAT requirements, unless the contractor requests SAT, or there is a compelling justification for requiring the training that is approved by the Contracting Officer (CO), in consultation with CSM. An example of this would be in an instance where a visually impaired employee is assigned to perform systems development and has potential staff-like access to IRS information.

(i) Security Orientation

All new contractor personnel must attend a system security orientation within the first 10 business days following initial assignment to any IRS contract, order, or agreement, and any additional IT SAT (commensurate with the individual's duties and responsibilities) within five business days of being granted access to an IRS, contractor, or subcontractor facility or system that processes IRS sensitive but unclassified (SBU) information. The Security Orientation will also be attended by new contractor personnel, including:

- Subcontractor personnel, who are authorized under contract to access IRS SBU information, IT systems, data; and
- Subcontractor personnel, who are authorized under contract to handle or access IRS SBU, contractor managed IT systems or IT assets used for performing IRS work, regardless of where work is performed.

(ii) Access to SBU Information and IT Systems SAT

Contractor personnel, including subcontractor personnel, required to complete SAT include, but are not necessarily limited to, those involved in any of the following activities:

- Manage, program or maintain IRS information in a production environment;
- Manage, program, or maintain IRS information in a development environment, either IRS owned or contractor owned/managed;
- Perform systems administration for either IRS systems or contractor managed resources, regardless of where IRS work is being performed;
- Operate an information system on behalf of the IRS on IRS systems or contractor (including subcontractor) managed systems;
- Conduct testing or development of information or information systems on behalf of the IRS on IRS systems or contractor (including subcontractor) managed systems;
- Provide advisory and assistance (consulting) services, or administrative support; or
- Handling, processing, access to, development, backup or any services to support IRS.

(iii)Service Personnel Security Awareness Training

Contractor personnel providing services in the following categories are required to complete Physical Security & Emergency Preparedness (PSEP) Training:

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

(iv)Service Personnel Inadvertent SBU Access Training

FAR §52.224-3 Privacy Training

PRIVACY TRAINING (JAN 2017)

(a) *Definition*. As used in this clause, "personally identifiable information" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (*See Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource*).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who–

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will–

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

Exhibit #3 (2 pages)

523-736
Conditional Access to Sensitive Information
Non-disclosure Agreement

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 the printing of the Freefile postcard and all its correspondence (including variable data). This approval will permit me conditional access to certain information, (taxpayers' personal information) 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 Internal Revenue Service. 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 Internal Revenue Service 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 Jacket 523-736 to ensure that no Internal Revenue Service 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 Internal Revenue Service 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 Internal Revenue Service 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 Internal Revenue Service 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 Internal Revenue Service 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 Jacket 523-736 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 Date

_____

Signature

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

_____ _____

IRS Contracting Officer's Representative Date