SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE OF
	1 57

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
TOFS-15-D-0001				

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	MARK GREEN		

9. ISSUED BY — CODE 1-IRS NON-IT

IRS non-IT (OTPA)
Internal Revenue Service
Mark C. Green 240-613-8444
6009 Oxon Hill Rd
Suite 700
Oxon Hill MD 20745

10. THIS ACQUISITION IS
- ☐ UNRESTRICTED OR ☒ SET ASIDE: 100.00 % FOR:
- ☐ SMALL BUSINESS
- ☐ HUBZONE SMALL BUSINESS
- ☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- ☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- ☐ EDWOSB
- ☒ 8(A)

NAICS: 541611
SIZE STANDARD: $15.0

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED ☐ SEE SCHEDULE	12. DISCOUNT TERMS	☐ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING / 14. METHOD OF SOLICITATION ☐RFQ ☐IFB ☐RFP

15. DELIVER TO — CODE

16. ADMINISTERED BY — CODE 1-IRS NON-IT (OT

IRS non-IT (OTPS)
Internal Revenue Service
6009 Oxon Hill Rd
Suite 700
Oxon Hill MD 20745

17a. CONTRACTOR/ OFFEROR — CODE 807372839 — FACILITY CODE

INTEGRATED FEDERAL SOLUTIONS INC.
1818 LIBRARY ST STE 500
RESTON VA 20190-6274

TELEPHONE NO.

18a. PAYMENT WILL BE MADE BY — CODE ARC/ASD/APB

ARC/ASD/APB
ARC/ASD/APB, AVERY 3G
www.ipp.gov

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Office of Financial Stability Acquisition Support Services Period of Performance: Base Year: 4/5/15 to 4/4/2016 Option Year 1: 4/5/16 to 4/4/2017 Period of Performance: 04/05/2015 to 04/04/2017				
0001	Senior Acquisition Analyst IAW Performance Work Statement for Term of Contract Continued ...		HR	[redacted]	
	(Use Reverse and/or Attach Additional Sheets as Necessary)				

25. ACCOUNTING AND APPROPRIATION DATA
See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*
$0.00

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.
☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☐ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

☒ 29. AWARD OF CONTRACT: _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR
[redacted]
Nicholas B. Dunn
2015.04.02 09:05:36 -04'00'

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
Mark C. Green
Digitally signed by Mark C. Green
DN: c=US, o=U.S. Government, ou=Department of the Treasury, ou=Internal Revenue Service, ou=People, serialNumber=716056, cn=Mark C. Green
Date: 2015.04.02 09:48:17 -04'00'

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
Nicholas Dunn, President & CEO	4-2-2015	MARK C. GREEN	

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
Prescribed by GSA - FAR (48 CFR) 53.212

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
0002	Mid-Level Acquisition Analyst IAW Performance Work Statement for Term of Contract		HR	[redacted]	
0003	Junior Acquisition Analyst IAW Performance Work Statement for Term of Contract		HR	[redacted]	
0004	Firm-Fixed Price task as specified in individual Task Order Performance Work Statement				
0005	Travel IAW Peformance Work Statement and individual Task Orders Not To Exceed amounts as specified. The total amount of award: $0.00. The obligation for this award is shown in box 26.				0.00

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

Acquisition Support Performance Work Statement
Office of Financial Stability:
Troubled Asset Relief Program

Background:

The Department of Treasury (Treasury) seeks to create an Indefinite Delivery Indefinite Quantity Contract (IDIQ) consistent with Federal Acquisition Regulation (FAR) Part 16 and SubPart 19.8. This contract will be a vehicle to satisfy recurring, repetitive requirements in an efficient and streamlined manner while also furthering agency goals of contracting with small, disadvantaged business concerns in the Small Business Administration's 8(a) Business Development Program.

Treasury requires acquisition support for the Office of Financial Stability's (OFS) Troubled Asset Relief Program (TARP). In 2008, the TARP Program was established by the Emergency Economic Stabilization Act to restore and maintain the liquidity and stability of America's financial system. The OFS acquisitions are primarily for professional legal, accounting, financial, and information technology services. As of July 2014 there have been over $4.7 billion obligated to OFS acquisitions. The OFS uses IDIQ contracts, Blanket Purchase Agreements, Simplified Acquisition Procedures, Federal Supply Schedule, and other procurement methods, as appropriate to meet mission needs. The OFS reports to various oversight bodies such as the Special Inspector General for TARP (SIGTARP), the Government Accountability Office (GAO), and Congress, which creates a need to maintain up to date information and reports in response to requests made by these authorities.

Scope:

The scope of this contract covers providing acquisition support for the OFS. This support includes assistance with contract data reporting, business process improvement, pre-award / post-award contract actions and input on functional design of internal procurement software tools and report automation.

Period of Performance:

The IDIQ period of performance will consist of a base year and one option year totaling a two year maximum period of performance. Task Orders will be issued as needed and state a period of performance.

Consistent with FAR Part 17, the Contracting Officer will review the vendor's performance and market pricing prior to the exercise of the option year to determine whether the contract still represents the best value.

Objectives:

1. Acquisition planning to include pre-award planning and documentation, market research, requirements development documents, quality assurance surveillance plans, synopses, source selection plans, solicitations, price negotiation memoranda, acquisition strategy support, etc.;

2. Acquisition management to include developing contract modifications, contract close-out assistance, assistance with reviewing contractor performance, etc.;

3. Acquisition data analysis and reporting to include contract data certifications, assist with reporting contract actions, assist with producing monthly, quarterly, and ad hoc contract data reports (e.g. high impact acquisitions, socio-economic data), etc.;

4. Document framework for current contracting processes, including analysis using current processes and reports to develop automation requirements and other efficiency savings and assist with defining future contract process and report automation requirements;

5. Assist with testing automation and providing formal documentation of results and recommended solutions;

6. Assist with the development of the Acquisition Management Solution (AMS) database structure and customized executive dashboards;

7. Assist with creating workflow designs utilizing the acquisition life cycle to track current procurement actions and pending actions;

8. Acquisition data verification and validation of reconciling OFS obligation dollars to Oracle on a monthly basis, to include resolving reconciliation and non-obligation accounting items to source documents on a monthly basis including resolving reconciliation breaks;

9. Assist with identifying improvement processes for OFS Contracting Officer's Representatives; and

10. Assist with updating current OFS acquisition policies and procedures to merge with new Contract Administration business processes.

11. Develop and update acquisition documentation, provide analyses, assessment, and recommendations, coordinate with stakeholders, conduct studies and analyses of required, current, and future acquisition requirements and track, validate, and report requirements activities using existing programs and databases.

Labor Category Requirements:

Labor Category	Required Education and Experience
Senior Acquisition Analyst	Twelve years of federal acquisition experience and bachelor's degree in business or a related field
Mid-Level Acquisition Analyst	Eight years of federal acquisition experience and bachelor's degree in business or a related field
Junior Acquisition Analyst	Four years of federal acquisition experience and bachelor's degree in business or a related field

Substitution Policy: Experience and education can be substituted on a year-for-year basis to meet requirements. For example, an individual with a master's degree in business and six years of acquisition experience would meet the requirements for a Mid-Level Acquisition Analyst.

Ordering Procedures:

A performance work statement, requisition with funding or an estimated cost, and any other necessary information must be submitted to the Contracting Officer for each project requirement and Task Order.

Contract Type:

Task Orders will be issued on either a firm-fixed price or labor hour basis.

IDIQ Contract Details:

IDIQ Contract Minimum guarantee: $5,000

Agency Ombudsman's information: Demetria Carter, Office of Procurement Policy Office of Procurement. 6009 Oxon Hill Road, Oxon Hill, MD. 240-613-8055

Ceiling / Purchase Limitation:

The cumulative value of all Orders under this contract shall not exceed the current 8(a) competitive threshold of $4,000,000.00, the maximum generally permitted for 8(a) sole source service acquisitions.

Funds are not obligated directly by the IDIQ. The IRS plans to, but does not promise, that funded Task Orders will be issued for specific work requirements during the course of the contract. Task Orders will provide critical support and address mission needs for the Treasury, OFS and IRS Office of Treasury Procurement Services.

Places of Performance:

Performance is expected to take place at one of the following locations (1) 1801 L Street, NW in Washington DC 20036, (2) 6009 Oxon Hill Road, Oxon Hill, MD 20745, or the contractor's facility. The contractor may be directed to work at other sites in the Washington DC metropolitan area.

Telework may be authorized by the Contracting Officer or the Contracting Officer's Representative due to situations such as inclement weather, building closures, and other events impacting agency needs. Upon request from the contractor's manager, the Contracting Officer or Contracting Officer's Representative may approve situational telework requests for individual contractor employees.

Government-Furnished Property:

When working on-site at a Government facility desk space and telephone / computer equipment will be provided.

Travel:

If required by Task Order(s), actual costs for travel pre-approved by the COR will be reimbursed in accordance with the Federal Travel Regulations and FAR Subpart 31.205-46 Travel Costs. Receipts or other appropriate documentation must accompany claims for reimbursement on travel expenses in excess of $75 in accordance with 41 CFR 301-52.15. Profit shall not be applied to travel costs. The total amount paid for travel on Task Orders shall not exceed the amounts Task Order Travel contract line items.

Section 508 Compliance:

The contractor shall comply with information technology accessibility requirements mandated by Section 508 of the Rehabilitation Act. Reports and documents produced must be accessible to persons with disabilities. Reference relevant contract clauses for detailed requirements.

Authority of Personnel:

The Contracting Officer, in accordance with Subpart 1.6 of the FAR, is the only person authorized to make or approve any changes in any of the requirements of this IDIQ contract and corresponding Task Orders. In the event the Contractor makes any changes at the direction of any person other than the Contracting Officer, the change will be considered to have been made without authority and no adjustment will be made in the Task Order price to cover any increase in cost incurred as a result thereof.

The authority of the COR is designated in DTAR Clause 1052.201-70 Contracting Officer's Representative (COR) Appointment and Authority.

Payment:

Invoices for work performed on Orders must be submitted electronically through the Invoice Processing Platform (IPP). Each invoice submitted shall be supported by appropriate documentation. Documentation necessary to substantiate an invoice shall include, but is not limited to, project name and number, invoice number, period of performance, percentage of work complete, original contract

amount, modification amounts, retainage amount and percent cumulative, labor categories, labor hours worked per labor category, labor rate, value of work in place, contractor's name, and contract number. Reference relevant contract clauses for detailed requirements.

Contractor Security:

On-site contractor personnel shall be subject to IRS and/or Treasury contractor security procedures depending on the place of performance. Reference relevant contract clauses for detailed requirements.

As required by the federal information security management act of 2002 (FISMA) and OMB guidance, the contractor personnel must complete both cyber security training and privacy awareness training within ten (10) days of commencing work pursuant to this contract. In addition, contractor personnel may be subject to background checks.

The Contractor shall ensure that all applicable personnel working on this contract and each Task Order, including subcontractors, meet the following security requirements for Contractors to protect against unauthorized disclosure of Sensitive But Unclassified (SBU) data. SBU data includes, but is not limited to, information that is protected from disclosure by the Privacy Act, 5 U.S.C. § 552a.

1) All applicable personnel shall be United States citizens or have lawful permanent resident status.

2) All applicable personnel shall be subject to a National Agency Check, Law and Credit (NACLC) investigation in accordance with the Department of the Treasury Security Manual (TD P 71-10). Applicable personnel shall not begin working on this contract and each Task Order until all security forms have been properly completed and submitted to Treasury for processing, as follows:

    a) Completed fingerprint cards
    b) Non-disclosure Agreement
    c) Fair Credit Reporting Act Release
    d) SF 85-P, “Questionnaire for Public Trust Positions”

3) Applicable personnel shall wear Treasury issued identification badges when working in Government facilities.

4) Applicable personnel, who undergo NACLC investigations that reveal, but are not limited to, the following, may be unacceptable under this contract: conviction of a felony, a crime of violence or a serious misdemeanor; a record of arrests for continuing offenses; or failure to file or pay Federal income tax. The Government reserves the right to determine if a Contractor employee assigned to a Task shall continue with the Task. The Contractor shall agree to remove the person assigned within one business day of official notification by the Government and provide a replacement within five business days. New hires or substitutions of personnel are subject to the NACLC investigation requirement.

Contracting Officer:

Mark C. Green
(240) 613-8444
Mark.green2@irs.gov

Data:

All data developed as a result of any work awarded under this contract is, and should remain, the property of the Federal Government.

Privacy:

Privacy: The provisions of the privacy act of 1974 protect Task information. All contractor personnel assigned to this Task shall take the proper precautions to protect the information from disclosure. Reference relevant contract clauses for detailed requirements.

Holidays:

The Department of the Treasury observes the following days as federal holidays.

January 1 New Year's Day
January Third Monday - Martin Luther King Day
February Third Monday - Washington's Birthday
May Last Monday - Memorial Day
July 4 Independence Day
September First Monday - Labor Day
October Second Monday - Columbus Day
November 11 Veterans Day
November Fourth Thursday - Thanksgiving Day
December 25 Christmas Day

Holiday observances of such days by Government personnel shall not be cause for additional period of performance or entitlement to compensation except as set forth in the contract. If the Offeror's personnel work on a holiday, no form of holiday or other premium compensation will be reimbursed either as a direct or indirect cost, unless authorized pursuant to an overtime clause elsewhere in the contract.

Key Personnel:

Personnel selected for Task Orders shall be key personnel. Task Orders shall include relevant Key Personnel clauses. The Contractor shall notify Treasury within 10 days regarding the departure of key personnel and provide a suitable replacement within 30 days of departure.

Non-performance of Inherently Governmental Functions:

This IDIQ contract and resultant Task Orders include services that are closely associated with inherently governmental functions. The contractor shall not perform any inherently governmental functions. Generally, the contractor may provide advice and draft documents, but not provide the

final decision/approval on matters relating to Treasury acquisitions. Contractor is prohibited from performing the activities listed in FAR 7.503. Further, contractor employees are expressly prohibited from receiving a warrant and serving as an agency Contracting Officer.

The contractor must notify all company employees working regularly in a government facility that questions regarding inherently governmental work can be directed to the Contracting Officer or COTR. The CO or COTR will advise on whether tasks are inherently governmental and provide technical direction on how to proceed. Further, contractor employees working regularly in a government facility must identify themselves as contractor employees (e.g. in their email signature lines).

Public-release contract version requirement:

This contract action utilizes TARP funds authorized by 110 P.L. 343. The program requires a high level of transparency and TARP contract documents are posted publicly at http://www.financialstability.gov or at another location designated by Treasury.

The Contractor agrees to submit to the CO and COR, within ten business (10) days from the date of award (exclusive of Saturdays, Sundays, and federal holidays), a .pdf file of the fully executed contract, blanket purchase agreement, or Order with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of the Treasury. The .pdf file must have searchable text and generally be compliant with the accessibility requirements in Section 508 of the Rehabilitation Act, 29 U.S.C. § 794(d). The Contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall demonstrate why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the Contractor in response to this requirement may itself be subject to disclosure under the FOIA.

The Treasury will carefully consider the entire Contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in the fully executed contract document may be properly withheld.

Quality Control:

The Contractor shall develop and maintain an effective quality assurance control program, including but not limited to a written Quality Control Plan, to ensure services are performed in accordance with this PWS. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor's quality control program is the means by which it assures itself that the work performed under the contract and task orders complies with the requirement of the contract. At a minimum, the Contractor shall develop written quality control procedures that address the areas identified in the "Performance Requirements Summary Matrix" set forth herein. Once the Quality Control Plan has been approved by the Contracting Officer in writing, changes to the Quality Control Plan can only be made after coordination with and written approval of the Contracting Officer.

Quality Assurance:

Treasury shall evaluate the Contractor's performance under this Order in accordance with the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused on what the Government must do to ensure that the Contractor has performed in accordance with the performance standards. Among other things, it defines how the performance standards will be applied, the frequency of surveillance.

Performance Requirements Summary Matrix

Performance Objective	Performance Standard	Acceptable Quality Levels	Government Surveillance	Remedy
Provide status updates on contract actions on workload tracker report.	Updates to must be made on a weekly basis.	Accuracy – No more than 5% of submitted reports require re-submission following Government review. Completeness – No more than 5% omission rate. Timeliness – 98% of reports submitted by the required due date.	100% review	Government will provide comments and Contractor will reconcile or incorporate all comments until documentation is acceptable.
Provide Required Contract Documentation	Contractor shall submit relevant contract file documentation to the Contracting Officer for signature as required.	Accuracy – No more than 3% of all submitted documentation requires re-submission following Contracting Officer's review. Completeness – Contractor is to provide all documentation pertinent to each contract action. No more than 2% omission rate. Timeliness – 98% of documentation submitted by the projected due date as identified on the weekly pipeline meetings.	100% review	Government will provide comments and Contractor will reconcile or incorporate all comments until documentation is acceptable.

COI Task Order Provisions:

CONFLICTS OF INTEREST

In addition to complying with COI Provisions in the underlying IDIQ contract regarding Conflicts of Interest, the Contractor shall sign a Task Order certification, and deliver it to the Treasury, prior to or simultaneously with the execution of each Task Order, in the form set forth in below.

Prior to beginning any work, any employee of the Contractor, its proposed subcontractors, and proposed consultants shall complete and sign Non-Disclosure Agreements.

TARP CONFLICTS OF INTEREST REGULATIONS

TASK ORDER CERTIFICATION FORMAT

I, [Name of Authorized Official], am a duly authorized official of [Name of Contractor] ("Contractor"). I have compared the Contractor's existing conflicts of interest mitigation plan ("Plan") submitted and approved by Treasury on (month/date/year) with the scope of work under the new Task Order [insert Task Order number] for work performed under Contract Number [insert contract number]. Based upon my review of the Plan, I certify that [check the one that applies]:

_____ No revisions/amendments are required to the Plan or;

_____ The Contractor has submitted a revised mitigation plan to Treasury that captures all or any necessary revisions or amendments to the Plan. Date submitted: _____

I also certify that the information provided in the Plan is complete and accurate in all respects as required under 31 C.F.R. Part 31.211(d).

Key individuals who are "personally and substantially" involved in performing work including subcontractors and consultants under this Task Order have provided written information to the Contractor regarding their personal, business and financial relationships as required under 31 C.F.R. Part 31.212(b).

Based upon the Contractor's reasonable knowledge and review of the information, I certify that key individuals [check the one that applies]:

_____ Do not have personal conflicts of interest, or

_____ Any and all personal conflicts of interest have been, voided, neutralized, or mitigated under the Contractor's Plan and any revisions/amendments to that Plan or has been waived by the Treasury. Attach description if applicable.

I confirm that key individuals have provided certifications to the Contractor that comply with the requirements in 31 C.F.R. Section 31.217(b), including any new key individuals who will perform work under this Task Order.

Based on my reasonable knowledge and review of the certifications obtained from the above key individuals as required under 31 C.F.R. Part 31.216(b), I certify that the Contractor and the above key individuals are aware of, and will comply with, the prohibitions set forth in 31 C.F.R. Section 31.216.

I confirm that the Contractor will make the information supporting this Task Order Certification available to Treasury upon request, and retain this information for three years following the termination or expiration of this Task Order.

[Name of Contractor]

By: _____

Name: _____

Title: _____

Date: _____

Conditional Access to Sensitive Information
Non-disclosure Agreement
Contract TOFS-15-D-0001 Task Order TBD

I, _____, hereby consent to the terms in this
(Print Name)
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 contract. This approval will permit me conditional access to certain 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 the Treasury Department, or in the case of bureau sensitive information released to the Office of Inspector General (OIG) or Treasury Inspector General for Tax Administration (TIGTA), or the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) in accordance with a written arrangement related to the official audit/investigative functions of the OIG or TIGTA or SIGTARP for that particular matter. 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 Treasury 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 the subject contract to ensure that no Treasury 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 Treasury 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 Treasury 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 Treasury 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 Treasury 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 the contract, 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 Treasury as a prior condition on conditional access to sensitive information. Further release to any other third party requires execution of a nondisclosure agreement.

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

NAME Date
TITLE, BUREAU/COMPANY

The following clauses are incorporated by reference:

FAR 52.219-1 Small Business Program Representations (Oct 2014)
FAR 52.212-4 Contract Terms and Conditions -- Commercial Items (Dec 2014)
(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Dec 2014)
(2) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).
____ Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104(g)).
(3) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).
(4) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77, 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the contracting officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

___ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).
___ (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Apr 2010) (41 U.S.C. 3509).
___ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub L. 111-5) (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009).
___ (4) 52.204-10, Reporting Executive compensation and First-Tier Subcontract Awards (Jul 2013) (Pub. L. 109-282) (31 U.S.C. 6101 note).
___ (5) [Reserved]
___ (6) 52.204-14, Service Contract Reporting Requirements (Jan 2014) (Pub. L. 111-117, section 743 of Div. C).
___ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Jan 2014) (Pub. L. 111-117, section 743 of Div. C).
___ (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Aug 2013) (31 U.S.C. 6101 note).
___ (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Jul 2013) (41 U.S.C. 2313).
__X_ (10) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (May 2012) (section 738 of Division C of Public Law 112-74, section 740 of Division C of Pub. L. 111-117, section 743 of Division D of Pub. L. 111-8, and section 745 of Division D of Pub. L. 110-161).
___ (11) (i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011) (15 U.S.C. 657a).
___ (ii) Alternate I (Nov 2011) of 52.219-3.
___ (12) (i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2011) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).
___ (ii) Alternate I (Jan 2011) of 52.219-4.
___ (13) [Reserved]
_X__ (14) (i) 52.219-6, Notice of Total Small Business Aside (Nov 2011) (15 U.S.C. 644).
___ (ii) Alternate I (Nov 2011).

___ (iii) Alternate II (Nov 2011).
___ (15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).
___ (ii) Alternate I (Oct 1995) of 52.219-7.
___ (iii) Alternate II (Mar 2004) of 52.219-7.
_X__ (16) 52.219-8, Utilization of Small Business Concerns (Oct 2014) (15 U.S.C. 637(d)(2) and (3)).
___ (17) (i) 52.219-9, Small Business Subcontracting Plan (Oct 2014) (15 U.S.C. 637 (d)(4)).
___ (ii) Alternate I (Oct 2001) of 52.219-9.
___ (iii) Alternate II (Oct 2001) of 52.219-9.
___ (iv) Alternate III (Oct 2014) of 52.219-9.
___ (18) 52.219-13, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).
_X__ (19) 52.219-14, Limitations on Subcontracting (Nov 2011) (15 U.S.C. 637(a)(14)).
___ (20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).
___ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011) (15 U.S.C. 657f).
__X_ (22) 52.219-28, Post Award Small Business Program Representation (Jul 2013) (15 U.S.C. 632(a)(2)).
___ (23) 52.219-29, Notice of Set-Aside for Economically Disadvantaged Women-Owned Small Business (EDWOSB) Concerns (Jul 2013) (15 U.S.C. 637(m)).
___ (24) 52.219-30, Notice of Set-Aside for Women-Owned Small Business (WOSB) Concerns Eligible Under the WOSB Program (Jul 2013) (15 U.S.C. 637(m)).
_X__ (25) 52.222-3, Convict Labor (June 2003) (E.O. 11755).
_X__ (26) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Jan 2014) (E.O. 13126).
_X__ (27) 52.222-21, Prohibition of Segregated Facilities (Feb 1999).
___ (28) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).
___ (29) 52.222-35, Equal Opportunity for Veterans (Jul 2014) (38 U.S.C. 4212).
_X__ (30) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).
___ (31) 52.222-37, Employment Reports on Veterans (Jul 2014) (38 U.S.C. 4212).
___ (32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
___ (33) 52.222-54, Employment Eligibility Verification (Aug 2013). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)
___ (34) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
___ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
___ (35) (i) 52.223-13, Acquisition of EPEAT® -Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514
___ (ii) Alternate I (Jun 2014) of 52.223-13.
___ (36) (i) 52.223-14, Acquisition of EPEAT® -Registered Television (Jun 2014) (E.O.s 13423 and 13514).
___ (ii) Alternate I (Jun 2014) of 52.223-14.

___ (37) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).
___ (38) (i) 52.223-16, Acquisition of EPEAT® -Registered Personal Computer Products (Jun 2014) (E.O.s 13423 and 13514).
___ (ii) Alternate I (Jun 2014) of 52.223-16.
_X__ (39) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (Aug 2011) (E.O. 13513).
__X_ (40) 52.225-1, Buy American--Supplies (May 2014) (41 U.S.C. chapter 83).
___ (41) (i) 52.225-3, Buy American--Free Trade Agreements--Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).
___ (ii) Alternate I (May 2014) of 52.225-3.
___ (iii) Alternate II (May 2014) of 52.225-3.
___ (iv) Alternate III (May 2014) of 52.225-3.
___ (42) 52.225-5, Trade Agreements (Nov 2013) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).
___ (43) 52.225-13, Restrictions on Certain Foreign Purchases (Jun 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
___ (44) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Jul 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
___ (45) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).
___ (46) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).
___ (47) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505), 10 U.S.C. 2307(f)).
___ (48) 52.232-30, Installment Payments for Commercial Items (Oct 1995) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).
_X__ (49) 52.232-33, Payment by Electronic Funds Transfer— System for Award Management (Jul 2013) (31 U.S.C. 3332).
___ (50) 52.232-34, Payment by Electronic Funds Transfer—Other Than System for Award Management (Jul 2013) (31 U.S.C. 3332).
___ (51) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).
___ (52) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).
___ (53) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).
___ (ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or executive orders applicable to acquisitions of commercial items:

___ (1) 52.222-41, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67.).
___ (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).
___ (3) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (Multiple Year and Option Contracts) (May 2014) (29 U.S.C.206 and 41 U.S.C. chapter 67).

___ (4) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).
___ (5) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67).
___ (6) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).
___ (7) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495).
___ (8) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792).
___ (9) 52.237-11, Accepting and Dispensing of $1 Coin (Sep 2008) (31 U.S.C. 5112(p)(1)).
___ (10) 52.222-55, Minimum Wages Under Executive Order 13658 Dec 2014)(Executive Order 13658).

(d) *Comptroller General Examination of Record* The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records -- Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.
(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.
(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.
(e)
(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Apr 2010) (41 U.S.C. 3509).
(ii) 52.219-8, Utilization of Small Business Concerns (Oct 2014) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $650,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.
(iii) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495). Flow down required in accordance with paragraph (1) of FAR clause 52.222-17.
(iv) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).
(v) 52.222-35, Equal Opportunity for Veterans (Jul 2014) (38 U.S.C. 4212).

(vi) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).
(vii) 52.222-37, Employment Reports on Veterans (Jul 2014) (38 U.S.C. 4212).
(viii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.
(ix) 52.222-41, Service Contract Labor Standards (May 2014), (41 U.S.C. chapter 67).
(x) 52.222-50, Combating Trafficking in Persons (Feb 2009) (22 U.S.C. 7104(g)).
___ Alternate I (Aug 2007) of 52.222-50 (22 U.S.C. 7104(g)).
(xi) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67.)
(xii) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67)
(xiii) 52.222-54, Employment Eligibility Verification (Aug 2013).
(xiv) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Jul 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
(xv) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.
(xvi) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.
(xvii) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2014)(Executive Order 13658).

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

52.233-1 – Disputes (May 2014)

The following clauses are incorporated by full text:

52.216-18 – Ordering (Oct 1995)
(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from date of contract award through four years following date of contract award.
(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.
(c) If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

52.216-19 -- Order Limitations (Oct 1995)
(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than $5,000, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.
(b) Maximum order. The Contractor is not obligated to honor --
(1) Any order for a single item in excess of $4M;
(2) Any order for a combination of items in excess of $4M; or
(3) A series of orders from the same ordering office within 30 days that together call for quantities exceeding the limitation in subparagraph (b)(1) or (2) of this section.
(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.
(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 30 days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of Clause)

52.216-22 -- Indefinite Quantity (Oct 1995)
(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.
(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."
(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.
(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after the expiration of the latest issues Task Order.

(End of Clause)

52.217-8 -- Option to Extend Services (Nov 1999)
The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days of expiration.

(End of Clause)

52.217-9 -- Option to Extend the Term of the Contract (Mar 2000)
(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.
(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed four years.

(End of Clause)

52.219-11 -- Special 8(a) Contract Conditions (Feb 1990)
The Small Business Administration (SBA) agrees to the following:
(a) To furnish the supplies or services set forth in this contract according to the specifications and the terms and conditions hereof by subcontracting with an eligible concern pursuant to the provisions of section 8(a) of the Small Business Act, as amended (15 U.S.C. 637(a)).
(b) That in the event SBA does not award a subcontract for all or a part of the work hereunder, this contract may be terminated either in whole or in part without cost to either party.
(c) Except for novation agreements and advance payments, delegate to the Department of the Treasury the responsibility for administering the subcontract to be awarded hereunder with complete authority to take any action on behalf of the Government under the terms and conditions of the subcontract; provided, however, that the Department of the Treasury shall give advance notice to the SBA before it issues a final notice terminating the right of a subcontractor to proceed with further performance, either in whole or in part, under the subcontract for default or for the convenience of the Government.
(d) That payments to be made under any subcontract awarded under this contract will be made directly to the subcontractor by the Department of the Treasury.
(e) That the subcontractor awarded a subcontract hereunder shall have the right of appeal from decisions of the Contracting Officer cognizable under the "Disputes" clause of said subcontract.
(f) To notify the Department of the Treasury Contracting Officer immediately upon notification by the subcontractor that the owner or owners upon whom 8(a) eligibility was based plan to relinquish ownership or control of the concern.

(End of Clause)

52.219-12 Special 8(a) Subcontract Conditions (Feb 1990)
(a) The Small Business Administration (SBA) has entered into Contract No. TOFS-15-D-0001 with the Department of Treasury to furnish the supplies or services as described therein. A copy of the contract is attached hereto and made a part hereof.
(b) IFS, hereafter referred to as the subcontractor, agrees and acknowledges as follows:

(1) That it will, for and on behalf of the SBA, fulfill and perform all of the requirements of Contract No. TOFS-15-D-0001 for the consideration stated therein and that it has read and is familiar with each and every part of the contract.

(2) That the SBA has delegated responsibility, except for novation agreements and advance payments, for the administration of this subcontract to the Department of Treasury with

complete authority to take any action on behalf of the Government under the terms and conditions of this subcontract.

(3) That it will not subcontract the performance of any of the requirements of this subcontract to any lower tier subcontractor without the prior written approval of the SBA and the designated Contracting Officer of the Department of Treasury.

(4) That it will notify the Department of Treasury Contracting Officer in writing immediately upon entering an agreement (either oral or written) to transfer all or part of its stock or other ownership interest to any other party.

(c) Payments, including any progress payments under this subcontract, will be made directly to the subcontractor by the Department of Treasury.

(End of Clause)

52.227-14 -- Rights in Data – General (May 2014)

(a) *Definitions.* As used in this clause--

"Computer database" or "database" means a collection of recorded information in a form capable of, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

"Computer software"—

(1) *Means*

(i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation.

"Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

"Form, fit, and function data" means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating, and attachment characteristics, functional characteristics, and performance requirements. For computer software it means data identifying source, functional characteristics, and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

"Limited rights" means the rights of the Government in limited rights data as set forth in the Limited Rights Notice of subparagraph (g)(2) if included in this clause.

"Limited rights data" means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications.

”Restricted computer software” means computer software developed at private expense and that is a trade secret; is commercial or financial and is confidential or privileged; or is copyrighted computer software, including minor modifications of the computer software.
“Restricted rights,” as used in this clause, means the rights of the Government in restricted computer software, as set forth in a Restricted Rights Notice of paragraph (g) if included in this clause, or as otherwise may be provided in a collateral agreement incorporated in and made part of this contract, including minor modifications of such computer software.
“Technical data” means recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computer databases (See 41 U.S.C. 116).
“Unlimited rights” means the right of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.
(b) *Allocation of rights*.

(1) Except as provided in paragraph (c) of this clause, the Government shall have unlimited rights in—

(i) Data first produced in the performance of this contract;
(ii) Form, fit, and function data delivered under this contract;
(iii) Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance and repair of items, components, or processes delivered or furnished for use under this contract; and
(iv) All other data delivered under this contract unless provided otherwise for limited rights data or restricted computer software in accordance with paragraph (g) of this clause.

(2) The Contractor shall have the right to—

(i) Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;
(ii) Use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, unless provided otherwise in paragraph (d) of this clause;
(iii) Substantiate use of, add or correct limited rights, restricted rights, or copyright notices and to take other appropriate action, in accordance with paragraphs (e) and (f) of this clause; and
(iv) Protect from unauthorized disclosure and use those data that are limited rights data or restricted computer software to the extent provided in paragraph (g) of this clause.

(c) *Copyright—*

(1) *Data first produced in the performance of this contract*.

(i) Unless provided otherwise in paragraph (d) of this clause, the Contractor may establish, without prior approval of the Contracting Officer, claim to copyright in scientific and technical articles based on or containing data first produced in the performance of this contract and published in academic, technical or professional journals, symposia proceedings or similar works. The prior, express written permission of the Contracting Officer is required to assert copyright in all other data first produced in the performance of this contract.

(ii) When authorized to assert copyright to the data, the Contractor shall affix the applicable copyright notices of 17 U.S.C. 401 or 402, and acknowledgment of Government sponsorship (including contract number).

(iii) For data other than computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable worldwide license in such copyrighted data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government. For computer software, the Contractor grants to the Government and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly (but not to distribute copies to the public) by or on behalf of the Government.

(2) *Data not first produced in the performance of this contract*. The Contractor shall not, without prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract unless the Contractor—

(i) Identifies the data; and

(ii) Grants to the Government, or acquires on its behalf, a license of the same scope as set forth in subparagraph (c)(1) of this clause or; if such data are restricted computer software, the Government shall acquire a copyright license as set forth in subparagraph (g)(4) of this clause (if included in this contract) or as otherwise provided in a collateral agreement incorporated in or made part of this contract.

(3) *Removal of copyright notices*. The Government will not remove any authorized copyright notices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.

(d) *Release, publication and use of data*. The Contractor shall have the right to use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, except—

(1) As prohibited by Federal law or regulation (*e.g.*, export control or national security laws or regulations);

(2) As expressly set forth in this contract; or

(3) If the Contractor receives or is given access to data necessary for the performance of this contract which contain restrictive markings, the Contractor shall treat the data in accordance with such markings unless otherwise specifically authorized otherwise in writing by the Contracting Officer.

(e) *Unauthorized marking of data*.

(1) Notwithstanding any other provisions of this contract concerning inspection or acceptance, if any data delivered under this contract are marked with the notices specified in paragraph (g)(3) or (g)(4) of this clause and use of the notices is not authorized by this clause, or if such data bears any other restrictive or limiting markings not authorized by this contract, the Contracting Officer may at any time either return the data to the Contractor, or cancel or ignore the markings. However, pursuant to 41 U.S.C. 4703, the following procedures shall apply prior to canceling or ignoring the markings.

(i) The Contracting Officer will make written inquiry to the Contractor affording the Contractor 60 days from receipt of the inquiry to provide written justification to substantiate the propriety of the markings;

(ii) If the Contractor fails to respond or fails to provide written justification to substantiate the propriety of the markings within the 60-day period (or a longer time approved in writing by the Contracting Officer for good cause shown), the

Government shall have the right to cancel or ignore the markings at any time after said period and the data will no longer be made subject to any disclosure prohibitions.

(iii) If the Contractor provides written justification to substantiate the propriety of the markings within the period set in subdivision (e)(1)(i) of this clause, the Contractor Officer will consider such written justification and determine whether or not the markings are to be canceled or ignored. If the Contracting Officer determines that the markings are authorized, the Contractor will be so notified in writing. If the Contracting Officer determines, with concurrence of the head of the contracting activity, that the markings are not authorized, the Contracting Officer will furnish the Contractor a written determination, which determination shall become the final agency decision regarding the appropriateness of the markings unless the Contractor files suit in a court of competent jurisdiction within 90 days of receipt of the Contracting Officer's decision. The Government shall continue to abide by the markings under this paragraph (e)(1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the Government will thereafter have the right to cancel or ignore the markings at any time and the data will no longer be made subject to any disclosure prohibitions), or by final disposition of the matter by court decision if suit is filed.

(2) The time limits in the procedures set forth in subparagraph (e)(1) of this clause may be modified in accordance with agency regulations implementing the Freedom of Information Act (5 U.S.C. 552) if necessary to respond to a request thereunder.

(3) Except to the extent the Government's action occurs as the result of final disposition of the matter by a court of competent jurisdiction, the Contractor is not precluded by paragraph (e) of this clause from brining a claim, in accordance with the Disputes clause of this contract, that may arise as a result of the Government removing or ignoring authorized markings on data delivered under this contract.

(f) *Omitted or incorrect markings*.

(1) Data delivered to the Government without any restrictive markings shall be deemed to have been furnished with unlimited rights. The Government is not liable for the disclosure, use, or reproduction of such data.

(2) If the unmarked data has not been disclosed without restriction outside the Government, the Contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of such data, permission to have authorized notices placed on qualifying data at the Contractor's expense, and the Contracting Officer may agree to do so if the Contractor—

(i) Identifies the data to which the omitted notice is to be applied;

(ii) Demonstrates that the omission of the notice was inadvertent;

(iii) Establishes that the use of the proposed notice is authorized; and

(iv) Acknowledges that the Government has no liability for the disclosure, use, or reproduction of any data made prior to the addition of the notice or resulting from the omission of the notice.

(3) If data has been marked with an incorrect notice, the Contracting Officer may—

(i) Permit correction of the notice at the Contractor's expense if the Contractor identifies the data and demonstrates that the correct notice is authorized, or

(ii) Correct any incorrect notices.

(g) *Protection of limited rights data and restricted computer software.*

(1) The Contractor may withhold from delivery qualifying limited rights data or restricted computer software that are not data identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause. As a condition to this withholding, the Contractor shall—

(i) Identify the data being withheld; and
(ii) Furnish form, fit, and function data instead.
(2) Limited rights data that are formatted as a computer database for delivery to the Government shall be treated as limited rights data and not restricted computer software.
(3) [Reserved]
(h) *Subcontracting*. The Contractor shall obtain from its subcontractors all data and rights therein necessary to fulfill the Contractor's obligations to the Government under this contract. If a subcontractor refuses to accept terms affording the Government such rights, the Contractor shall promptly notify the Contracting Officer of the refusal and shall not proceed with the subcontract award without authorization in writing from the Contracting Officer.
(i) *Relationship to patents or other rights*. Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government.

(End of Clause)

FAR 52.252-2 -- Clauses Incorporated by Reference (Feb 1998)
This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):
http://farsite.hill.af.mil/farsite.html

(End of Clause)

1052.219–72 8(A) Business development program awards (Jun 2003)
(a) This purchase/delivery/Task Order or contract is issued by the contracting activity directly to the 8(a) program participant/ contractor pursuant to the Partnership Agreement between the Small Business Administration (SBA) and the Department of the Treasury. However, the Small Business Administration is the prime contractor and retains responsibility for 8(a) certification, 8(a) eligibility determinations and related issues, and provides counseling and assistance to the 8(a) contractor under the 8(a) Business Development program. The cognizant SBA district office is: Washington D.C.

(b) The contracting officer is responsible for administering the purchase/delivery/Task Order or contract and taking any action on behalf of the Government under the terms and conditions of the purchase/delivery/Task Order or contract, to include providing the cognizant SBA district office with a signed copy of the purchase/delivery/Task Order or contract award within 15 days of the award. However, the contracting officer shall give advance notice to the SBA before it issues a final notice terminating performance, either in whole or in part, under the purchase Order or contract. The contracting officer shall also coordinate with SBA prior to processing any novation agreement. The contracting officer may assign contract administration functions to a contract administration office.

(c) The contractor agrees:
(1) to notify the contracting officer, simultaneously with its notification to SBA (as required by SBA's 8(a) regulations), when the owner or owners upon whom 8(a) eligibility is based, plan to relinquish ownership or control of the concern. Consistent with 15 U.S.C.37(a)(21), transfer of ownership or control shall result in termination of the contract for convenience, unless SBA waives the requirement for termination prior to the actual relinquishing of control; and,
(2) to adhere to the requirements of FAR 52.219–14, Limitations on Subcontracting.

(End of clause)

1052.201–70 Contracting Officer's Representative (COR) appointment and Authority (AUG 2011)

(a)

The COR is:
Rebeckah Schlosser
(202) 927-0841
Rebeckah.Schlosser@treasury.gov

The Alternate COR is:
Denise Pope
(202) 927-9403
Denise.Pope@treasury.gov

(b) Performance of work under this con- tract is subject to the technical direction of the COTR identified above, or a representa- tive designated in writing. The term ''technical direction'' includes, without limitation, direction to the contractor that directs or redirects the labor effort, shifts the work between work areas or locations, and/or fills in details and otherwise serves to ensure that Tasks outlined in the work statement are accomplished satisfactorily.
(c) Technical direction must be within the scope of the contract specification(s)/work statement. The COTR does not have authority to issue technical direction that:
(1) Constitutes a change of assignment or additional work outside the contract specification(s)/work statement;
(2) Constitutes a change as defined in the clause entitled ''Changes'';
(3) In any manner causes an increase or decrease in the contract price, or the time required for contract performance;
(4) Changes any of the terms, conditions, or specification(s)/work statement of the contract;
(5) Interferes with the contractor's right to perform under the terms and conditions of the contract; or
(6) Directs, supervises or otherwise controls the actions of the contractor's employees.
(d) Technical direction may be oral or in writing. The COTR must confirm oral direction in writing within five workdays, with a copy to the Contracting Officer.
(e) The Contractor shall proceed promptly with performance resulting from the technical direction issued by the COTR. If, in the opinion of the contractor, any direction of the COTR or the designated representative falls within the limitations of (c) above, the contractor shall immediately notify the Contracting Officer no later than the beginning of the next Government work day.
(f) Failure of the Contractor and the Contracting Officer to agree that technical direction is within the scope of the contract shall be subject to the terms of the clause entitled ''Disputes.''

(End of clause)

1052.232–7003 Electronic submission of payment requests.
(a) Definitions. As used in this clause—
(1) ‘‘Payment request’’ means a bill, voucher, invoice, or request for contract financing payment with associated supporting documentation. The payment request must comply with the requirements identified in FAR 32.905(b), ‘‘Payment documentation and process’’ and the applicable Payment clause included in this contract.
(2) [Reserved]
(b) Except as provided in paragraph (c) of this clause, the Contractor shall submit payment requests electronically using the Internet Payment Platform (IPP). Information regarding IPP is available on the Internet at www.ipp.gov. Assistance with enrollment can be obtained by contacting the IPP Production Helpdesk via email ippgroup@bos.frb.org or phone (866) 973–3131.
(c) The Contractor may submit payment requests using other than IPP only when the Contracting Officer authorizes alternate procedures in writing.
(d) If alternate payment procedures are authorized, the Contractor shall include a copy of the Contracting Officer’s written authorization with each payment request.

(End of clause)

DTAR 1052.222–70: Minority and Women Inclusion (April 2014)
Contractor confirms its commitment to equal opportunity in employment and contracting. To implement this commitment, the Contractor shall ensure, to the maximum extent possible consistent with applicable law, the fair inclusion of minorities and women in its workforce. The Contractor shall insert the substance of this clause in all subcontracts awarded under this Contract whose dollar value exceeds $150,000. Within ten business days of a written request from the contracting officer, or such longer time as the contracting officer determines, and without any additional consideration required from the Agency, the Contractor shall provide documentation, satisfactory to the Agency, of the actions it (and as applicable, its subcontractors) has undertaken to demonstrate its good faith effort to comply with the aforementioned provisions. For purposes of this contract, ‘‘good faith effort’’ may include actions by the contractor intended to identify and, if present, remove barriers to minority and women employment or expansion of employment opportunities for minorities and women within its workforce. Efforts to remove such barriers may include, but are not limited to, recruiting minorities and women, providing job-related training, or other activity that could lead to those results. The documentation requested by the contracting officer to demonstrate ‘‘good faith effort’’ may include, but is not limited to, one or more of the following:

1. The total number of Contractor’s employees, and the number of minority and women employees, by race, ethnicity, and gender (e.g., an EEO–1);
2. A list of subcontract awards under the Contract that includes: dollar amount, date of award, and subcontractor’s race, ethnicity, and/or gender ownership status;
3. Information similar to that required in item 1, above, with respect to each subcontractor; and/or

1. The Contractor’s plan to ensure that minorities and women have appropriate opportunities to enter and advance within its workforce, including outreach efforts. ‘‘Consistent with Section 342(c)(3) of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Pub. L. 111–203)(Dodd-Frank Act), a failure to demonstrate to the Director of the Agency’s Office of Minority and Women Inclusion such good faith efforts to include minorities and women in the Contractor’s workforce (and as applicable, the workforce of its subcontractors), may result in termination of the Contract for default, other contractual remedies, or referral to the Office of Federal Contract Compliance

Programs. Compliance with this clause does not, however, necessarily satisfy the requirements of Executive Order 11246, as amended, nor does it preclude OFCCP compliance evaluations and/or enforcement actions undertaken pursuant to that Order. ‘‘For purposes of this clause, the terms ‘‘minority,’’ ‘‘minority-owned business’’ and ‘‘women-owned business’’ shall have the meanings set forth in Section 342(g) of the Dodd-Frank Act.

(End of clause)

IR1052.239.9010 Section 508 Services (Sep 2006)
All contracts, solicitations, purchase Orders, delivery Orders and interagency agreements that contain a requirement of services which will result in the delivery of a new or updated electronic and information technology (EIT) item/product must conform to the applicable provisions of the appropriate technical standards in 36 CFR 1194, Subpart B, and functional performance criteria in 36 CFR 1194.31, Subpart C, unless an agency exception to this requirement exists.

The following technical standards and provisions have been determined to be applicable to this contract:

___ 1194.21, Software applications and operating systems.
__(a) __(b) __(c) __(d) __(e) __(f) __(g) __(h)
__(i) __(j) __(k) __(l)

_X_ 1194.22, Web-based intranet and internet information and applications.
_x_(a) _x_(b) _x_(c) _x_(d) _x_(e) _x_(f) _x_(g) _(h) _x_(i) _x_(j)
_x_(k) _x_(l) _x_(m) __(n) _x_(o) _x_(p)

___ 1194.23, Telecommunications products.
__(a) __(b) __(c) __(d) __(e) __(f) __(g) __(h) __(i) __(j)
__(k:1) __ (k:2) __(k:3) __(k:4)

___ 1194.24, Video and multimedia products.
__(a) __(b) __(c) __(d) __(e)

___ 1194.25, Self contained, closed products.
__(a) __(b) __(c) __(d) __(e) __(f) __(g) __(h) __(i) __(j)

___ 1194.26, Desktop and portable computers.
__(a) __(b) __(c) __(d)

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

The following functional performance criteria (36 CFR 1194.31) apply to this contract.

_X_ (a) At least one mode of operations and information retrieval that does not require user vision shall be provided, or support for assistive technology used by people who are blind or visually impaired shall be provided.

_X_ (b) At least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 shall be provided in audio and enlarged print output working together or independently, or support for assistive technology used by people who are visually impaired shall be provided.

_X_ (c) At least one mode of operation and information retrieval that does not require user hearing shall be provided, or support for assistive technology used by people who are deaf or hard of hearing shall be provided.

_X_ (d) Where audio information is important for the use of a product, at least one mode of operation and information retrieval shall be provided in an enhanced auditory fashion, or support for assistive hearing devices shall be provided.

_X_ (e) At least one mode of operation and information retrieval that does not require speech shall be provided, or support for assistive technology used by people with disabilities shall be provided.

(End of clause)

IR1052.239-9008 Section 508 – Information, Documentation, and Support (Sep 2006)
In accordance with 36 CFR 1194, Subpart D, the electronic information technology (EIT) products and product support services furnished in performance of this contract shall be documented to indicate the current conformance level with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board s Electronic and Information Technology Accessibility Standards. At no time during the performance of the award shall the level of conformance go below the level of conformance in place at the time of award. At no additional cost, the contractor shall provide information, documentation, and support relative to the supplies and services as described
in the statement of work. The contractor shall maintain this detailed listing of compliant products for the full contract term, including forms of extensions, and shall ensure that it is current within five calendar days after award and within three calendar days of changes in products being utilized as follows:

(a) Product support documentation provided to end-users shall be made available in alternate formats upon request, at no additional charge.

(b) End-users shall have access to a description of the accessibility and compatibility features of products in alternate formats or alternate methods upon request, at no additional charge.

(c) Support services for products shall accommodate the communication needs of end-users with disabilities.

(End of clause)

IR1052.204-9003 - IRS Security Awareness Training Requirements (Jun 2013)
The Federal Information Security Management Act of 2002 (FISMA) requires each federal agency to provide periodic information security awareness training to all employees, including contractors, involved in the management, use, or operation of Federal information and information systems. In addition, IRS contractors 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 shall ensure all contractor 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 CSM@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 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, in consultation with CSM.***

(i) Security Orientation
All new contractor personnel shall attend a system security orientation within the first 10 business days following initial assignment to any IRS contract/Order, and additional IT security awareness training (commensurate with the individual's duties and responsibilities) within 5 business days of being granted access to an IRS facility or system. The Security Orientation will also be attended by new contractor personnel, including subcontractor personnel, who are authorized under contract to access IRS IT systems, data, and assets from or through contractor-managed facilities, systems, and assets, including laptop computers, workstations, servers, and other IT resources.
(ii) Access to Sensitive but Unclassified (SBU) Information and IT Systems Security Awareness Training (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;
- Operate an information system on behalf of the IRS;
- Conduct testing or development of information or information systems on behalf of the IRS;
- 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 Training:
- Medical;
- Cafeteria;
- Landscaping;
- Janitorial and cleaning (daylight operations);
- Building maintenance; or
- Other maintenance and repair.

(iv) Service Personnel Inadvertent SBU Access Training
Contractor personnel performing: (i) janitorial and cleaning services (daylight operations), (ii) building maintenance, or (iii) other maintenance and repair and need access to IRS facilities and building wherein pipeline processing (the processing of paper tax returns) is performed or where the facility and building has an exemption to the clean desk policy authorized by PSEP, are required to complete Inadvertent SBU Access training. Facilities performing pipeline processing and/or have an exemption to the clean desk policy are:

Clean Desk Waiver Facilities: (Note: The facilities listed below could change annually and are only authorized for one year.)
- KY2032 333 Scott St., Covington, KY 41001
- KY3005 300 Madison Ave., Covington, KY 41011
- MI1951 985 Michigan Ave., Detroit, MI 48226
- MN1600 30 East Seventh St., St. Paul, MN 55101
- TX2225 2191 Woodward St., Austin, TX 78744

Pipeline Processing Facilities:
- CA4664 Fresno Campus, 5045 E. Butler, Fresno, CA 93727
- CA7370 1950 G Street, Fresno, CA 93706
- CA6530 1000 N. Mooney St., Tulare, CA 93274
- KY0085 Covington Campus, 200 West Fourth St., Covington, KY 41011
- KY3016 7125 Industrial Rd., Florence, KY 41042
- MO1937 Kansas City Campus, 33 W. Pershing Rd., Kansas City, MO 64108
- TX2038 Austin Campus, 3651 S IH-35, Austin TX 78741
- TX2746 5015 S IH-35, Austin TX 78741
- UT0036 Ogden Campus, 1160 W 1200 S, Ogden, UT 84409
- UT1430 1973 North Rulon White Blvd., Ogden, UT 84404
- UT1476 1125 W 12th St., Ogden, UT 84201

(v) Training Certificate/Notice
The contractor shall submit confirmation of completed SAT (using the form at the Mandatory Briefing web site) or via a confirmation email to CSM at CSM@irs.gov for each employee assigned to a contract/Order subject to this clause, with a copy to the Contracting Officer and Contracting Officer's Representative (COR), upon completion, but not later than 10 business days after starting performance under the contract/Order. If required by the COR, the contractor may be required to input data into a system, to be defined by the IRS, to describe the security controls being used to protect information, including confirmation of security awareness training.

(vi) Annual Training
For contracts/Orders exceeding one year in length, either on a multiyear or multiple year basis, contractor must ensure that personnel complete SAT annually not later than April 30th of each year. The contractor shall submit confirmation of completed annual SAT on all personnel assigned to this contract/Order, via email, to the CO, COR, and CSM upon completion, but not later than May 12th of the then current calendar year or as requested by CSM (whichever date is earlier).

b. SAT is available on the Mandatory Briefing web site or if this site is not accessible, SAT materials will be made available by CSM at CSM@irs.gov.

c. Contractor's failure to comply with IRS security policy (to include completion and certification of SAT requirements within the timeframe specified) may be subject to having access to IRS IT systems and facilities suspended, revoked or terminated (temporarily or permanently).

(End of clause)

IR1052.204-9005 Submission of Security Forms and Related Materials (Jun 2013)
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 must undergo security investigative processing appropriate to the position sensitivity and risk level designation associated to determine whether the Contractor personnel should be permitted to work in the identified position. For security requirements at contractor facilities using contractor managed resources, please reference Publication 4812, Contractor Security Controls.

a. Contractor personnel performing under an agreement that authorizes unescorted access to and in IRS facilities, and access to Sensitive But Unclassified (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;
(2) Selective Service registration compliance;
(3) U.S. citizenship/residency compliance;
(4) Background investigation forms;
(5) Credit report results (moderate and high risk investigations only);
(6) Federal Bureau of Investigation fingerprint results; and
(7) If applicable, prior background investigations.

In this regard, Contractor shall furnish the following electronic documents to the Contractor Security Management (CSM) at CSM@irs.gov or CSLP@irs.gov within 10 business days of assigning (or reassigning) an employee to this contract/Order and *prior* to the contract employee performing any work thereunder:

- The IRS provided Risk Assessment Checklist (RAC), and

- All required security forms (for new contractor employees), are available through the publicly accessible website for IRS Procurement.

b. Tax Compliance, Credit Checks and Fingerprinting:
(1) Contractor personnel whose contract/Order exceeds 180 days must be eligible for access, per certification of tax compliance, and shall undergo, at a minimum a National Agency Check and Inquiries as a condition of work under the contract/Order, to include a credit check and fingerprinting.
(2) If the duration of employment is less than 180 days or access is infrequent (e.g., 2-3 days per month) and the contractor requires unescorted access, the contractor employee must be eligible for access, per certification of tax compliance, and require at a minimum a fingerprint check (Special Agreement Check).
(3) With the exception of contractors who need access to IT systems, no background investigation or tax check is necessary if the duration of employment is less than 180 days or access is infrequent when there is escort provided by an IRS employee or an approved contractor employee at the same or higher position risk level.
The contractor employee will be permitted to perform under the contract and have access to IRS facilities only upon notice of an interim or final approval, as defined in Internal Revenue Manual (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, IRM 10.2.14 – Methods of Providing Protection, and IRM 10.8.1 - Policy and Guidance.
As prescribed in IRM 10.23.2, escorting in lieu of staff-like access for IT systems will not be allowed.

(End of clause)

IR1052.204-9006 Notification of Change in Contractor Employee Employment Status, Assignment, or Standing (Jun 2013)

The contractor shall notify the Contracting Officer's Representative (COR) and the Contractor Security Management (CSM), via email to CSM@irs.gov, within 1 business day of the contractor becoming aware of any change in the employment status, assignment, or standing of a contractor employee to this contract/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 IRS contract/Task Order;
- Knowledge of the employee's voluntary separation from employment or performance on this contract/Task Order (if no prior notice was given);
- Transfer or reassignment of the employee and performance of duties under this contract/Task Order, in whole or in part, to another IRS contract/Task Order (*and identify the gaining contract and representative duties/responsibilities to allow for an assessment of suitability based on position sensitivity/risk level designation*);
- 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/Task Order (*provide explanation*);
- Death.

When required by the COR, the contractor may be required to provide the information required by this clause to the IRS using the Archer application or similar application that will be used also to track security performance.

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/Task Order number(s)
- Actual or anticipated date of departure or separation
- When applicable, the name of the IRS facility(s) this individual routinely works from or has access to when performing work under this contract/Order
- When applicable, contractors using contractor owned systems for IRS 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.
- 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 employee is working on multiple contracts/Orders, notification shall be combined, and the cognizant COR for each affected contract/Order 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.)

As a general rule, the change in the employment status, assignment, or standing of a contractor personnel to this contract/Order would not form the basis for an excusable delay for failure to perform this contract under its terms.

(End of clause)

IR1052.239-9007 Access, Use or Operation of IRS Information Technology (IT) Systems by Contractors (Jun 2013)

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

1. IRS Information Technology Security Policy and Guidance. All current and new IRS contractor employees authorized staff-like (unescorted) access to Treasury/IRS owned or controlled facilities and information systems, or work, wherever located, on those contracts which involve the design, operation, repair or maintenance of information systems and access to sensitive but unclassified information shall comply with the IRS Information Technology Security Policy and Guidance, Internal Revenue Manual (IRM) 10.8.1 and IRS Publication 4812. A copy of IRM 10.8.1 is available at http://www.irs.gov/irm/. This requirement applies to contractors who are performing under contract using contractor-managed systems, including laptop computers, workstations, servers, and other IT resources) at contractor managed facilities. A copy of Publication 4812 is available at http://www.irs.gov/uac/Procurement.

2. Access Request and Authorization. Within ten (10) business days after contract award or issuance of an Order, the contractor shall provide the COR and the Contractor Security Management (CSM), via email to CSM@irs.gov, a list of names of all applicable contractor and subcontractor employees and the IRS location(s) identified in the contract for which access is requested. A security screening, if determined appropriate by the IRS and in accordance with IRM 10.23.2, Contractor Investigations, and Department of the Treasury Security Manual (TD P) 15-71, Chapter II, Section 2, will be conducted by CSM. Upon notification of a favorable adjudication of a security screening, the COR will complete an Online 5081 (OL 5081), Automated Information System (AIS) User Registration/Change Request, for each prime or subcontractor employee and require an electronic signature from each such employee indicating the contractor employee has read and fully understands the security requirements governing access to the Service's IT systems.

3. Remote Access. If the contract authorizes access to IRS IT systems, information, or assets remotely; that is, from the contractor or other facility, office, or site, the requirements of this clause governs, as well as the general guidance and specific security control standards in IRS Publication 4812, Contractor Security Controls. 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.

4. Contractor Acknowledgement. The contractor also acknowledges and agrees: (a) That employees must comply with all laws, IRS system security rules and security policies, standards, and procedures, and (b) That any one of its employees unsanctioned, negligent, or willful violation of the laws, system security rules, and security policies, standards, and procedures may result in the revocation of access to IRS information technology systems, immediate removal from IRS premises and the contract, and may be subject to arrest by Federal law enforcement agents.

5. Limited Personal Use of Government IT Resources.

a. Contractors, like Federal employees, have no inherent right to use Government IT resources and this policy does not create the right to use Government IT resources for nonGovernmental purposes.

See RM 10.8.27, Exhibit 10.8.27-1, Prohibited Uses of Government IT Resources, for specific examples of prohibited uses. See Title 5 - Code of Federal Regulations (CFR) - Part 734 – Political Activities of Federal Employees, for specific examples of prohibited political activities.
b. Any unauthorized use must be reported –within the first hour that it becomes known that an incident has occurred—to the COR, the Contracting Officer, and Situation Awareness Management Center (SAMC). SAMC shall be contacted by telephone at (866) 216-4802) or TTY at 800-877-8339.
 Information about unclassified cyber security incidents of a sensitive nature shall be transmitted using secure messaging or alternative forms of encryption.

 If the incident involves the loss, misuse, or unauthorized inspection of Sensitive but Unclassified (SBU) information, the contractor shall also report the incident/situation to the Treasury Inspector General for Tax Administration (TIGTA) hotline at 800-366-4484.

6. Replacement Personnel.
The CO, at his/her discretion, may require removal of the employee from performance under this or any IRS contract and may require replacement personnel with similar credentials within 5 days of the notice to remove. Replacement personnel must be acceptable to the CO, in consultation with the COR.

7. Monitoring Notification.
IRS management retains the right to monitor both the content and the level of access of contractor employees' use of IRS IT systems. Contractor employees do not have a right, nor should they have an expectation, of privacy while using any IRS information technology system at any time, including accessing the Internet or using e-mail.

8. Security Reports and Information.
If any reports are required, the COR may direct the submission of such reports and information through a specific IRS application, to be determined, or the entry of specific information into the application or system.

9. Subcontracts.
The Contractor shall incorporate this clause in all subcontracts, subcontract Task or delivery Orders or other subcontract performance instrument where the subcontractor employees will require access, use or operation of IRS information technology systems.

(End of clause)

IR1052.224-9008 – Safeguards Against Unauthorized Disclosure of Sensitive but Unclassified Information (Oct 2012)
In performance of this contract, the contractor agrees to comply with the following requirements and assumes responsibility for compliance by its employees and subcontractors, as applicable:

(a) *Definitions*. As used in this clause—

"Information," as defined by OMB Circular A-130 – Management of Federal Information Resources, means "any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms."

"Sensitive But Unclassified," as described in the Department of the Treasury Security Manual (Treasury Directive Publication 15-71 (TD P 15-71), Chapter III – Information Security, Section 24 – Sensitive But Unclassified Information), is a term that ". . . originated with the Computer Security Act of 1987. It defined SBU 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.'"

Furthermore, "SBU shall be the primary term used to mark sensitive information originating in the Departmental Offices (DO)/bureaus. . . . Access to SBU shall be based on a determination that an employee, contractor personnel or consultant requires access to specific SBU information in Order to perform or assist in lawful, authorized DO/bureau Governmental functions . . ."[1]

SBU information may be categorized in one or more of the following groups—

(1) **Returns and Return Information**

Includes all information protected by § 6103 of the Internal Revenue Code (IRC), 26 U.S.C. § 6103.

(2) **Sensitive Law Enforcement Information**

Includes grand jury, informant, and undercover operations information.

(3) **Employee Information**

Includes all employee information covered by the Privacy Act of 1974 (5 U.S.C. 552A (g)(1), as amended Examples include personnel, payroll, job applications, disciplinary actions, performance appraisals, drug tests, health exams and evaluation data.

(4) **Personally Identifiable Information (PII)**

Includes the uniquely identifiable personal information of taxpayers, employees, contractors, applicants, and visitors to the IRS. However, names of federal employees when used for business purposes, along with employee business phone numbers and business addresses are all considered publicly available information. Examples of PII include, but are not limited to—

- Name;
- Home address;
- Social Security Number;

[1] For any pertinent Government publication or document that uses the term "Controlled Unclassified Information (CUI)," or the term "sensitive information," either term, for the purposes of this clause, may be considered equivalent to and have the same meaning as "SBU information."

- Date of birth;
- Home telephone number;
- Biometric data (e.g., height, weight, eye color, fingerprints, etc.); and
- Other numbers or information that alone or in combination with other data can identify an individual, or other personal information which is linked or linkable to an individual and can be used to distinguish or trace an individual's identity.

(5) **Other Protected Information**

Includes all information covered by the Trade Secrets Act (18 U.S.C. 1905), the Procurement Integrity Act (41 U.S.C. 423) (P.L. 111-350), and similar statues. Examples include, but are not limited to—

- Information considered procurement sensitive;
- Information marked Limited Official Use (LOU);
- Information marked Official Use Only (OUO);
- Law Enforcement Manuals (LEM)
- Records about individuals requiring protection under the Privacy Act;
- Information that is not releasable under the Freedom of Information Act (FOIA);
- Proprietary data (business information that does not belong to the IRS);
- Procurement sensitive data, such as contract proposals;
- Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on Government contracts, or disclosure of proprietary information entrusted to the Government; or
- Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities; and
- Other protected information includes information, which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission. For contracting organizations providing IT support to the IRS, this includes specific IT configurations, where the system security configurations could identify the state of security of that system; IP addresses that allow the workstations and servers to be potentially targeted and exploited; and source code that reveals IRS processes that could be exploited to harm IRS programs, employees or taxpayers.

"Live Data" is another form of Other Protected SBU information. It is primarily unmodified, non-sanitized data extracted from taxpayer files which identities specific individuals or corporate taxpayers. It includes taxpayer information, tax return information, live employee data, PII, and other SBU information that is used outside of the authorized IRS production environment. The use of live data in testing environments is limited to tax administration or other authorized IRS purposes and may be disclosed only to those individuals with a need to know. The use of live data is strictly prohibited without approval from Privacy, Governmental Liaison and Disclosure (PGLD), Privacy and Information Protection, Privacy, Privacy Compliance and shall only be considered when it is impossible to create effective synthetic data, and then only in strict compliance with IRM 10.8.8 – Information Technology (IT) Security, Live Data Protection.

"IRS records or information" (or simply IRS information), as described in IRM 11.3.35 – Requests and Demands for Testimony and Production of Documents, mean "any material (including copies thereof) contained in the files (including paper, electronic, or other media files) of the IRS, any information relating to material contained in the files of the IRS, or any information acquired by a current or former IRS officer, employee, or contractor, while an IRS officer, employee, or contractor as a part of the performance of official duties or because of that IRS officer's, employee's, or contractor's official status with respect to the administration of the internal revenue laws or any other laws administered by or concerning the IRS."

(b) *Conditional or Controlled Release*.

(1) For solicitations— When the disclosure or release of returns, return information, or other SBU information is required to enable prospective offerors to fully evaluate the parameters of the work involved for a specific requirement, as allowed under IRM 11.3.24.5 (and such release has been pre-approved by the Business Operating Division (the Requisitioner) and concurred upon one level above the Contracting Officer (in consultation with Personnel Security, or the PGLD, Office of Privacy, or other appropriate organizational units)), prospective offerors shall be subject to this and any related Safeguard or Privacy Act clauses or provisions of the solicitation, and any related security controls or security restrictions and limitations described in the solicitation. Before or at the time of disclosure or release of returns, return information, or other SBU information during the solicitation phase of the acquisition, the IRS may determine that a pre-award on-site security inspection needs to be performed as a condition for disclosure or release. The solicitation will describe the steps to be taken if and when such an on-site security inspection is to be performed.

When the IRS intends to issue a solicitation containing SBU information (and approved for release), it will usually accomplish this through the Governmentwide Point of Entry (GPE) as transmitted via Federal Business Opportunities (also referred to as FedBizOpps or FBO). At FedBizOpps, a solicitation that does not contain sensitive information (and that is customarily available to the general public) is, in effect, a "FBO Solicitation." Whereas, a solicitation that contains SBU information or controlled, unclassified documents (and is available only to authorized, registered users) is referred to by FedBizOpps as a "Non-FBO Solicitation." Agency "buyers" can upload non-sensitive documents (and attach existing controlled, unclassified documents to notices) and create Non-FBO solicitation links that create document packages that are not tied to FBO solicitations (parallels functionality previously found in the FedTeDS (Federal Technical Data Solutions), a defunct password-protected, web-based tool designed to safeguard the distribution of sensitive, unclassified, acquisition-related information for all federal agencies). The link then takes the vendor to a system interface where their authorization to review materials (explicit access / export controlled) is vetted prior to letting the vendor access the materials. A Government user can pro-actively select a vendor user for access, or a vendor can request, and be granted access, through this system. Before a vendor registers in FBO, it will need to obtain a Data Universal Numbering System (DUNS) Number. The DUNS Number is assigned by Dun & Bradstreet, Inc. (D&B) to identify unique business entities, and is obtained via the Central Contractor Registration (CCR) system accessed through the System for Award Management (SAM). When an explicit access or export control request is initiated, the Non-FBO system retrieves a vendor's profile information directly from CCR/SAM.

Once the vendor is given explicit access to review the package, they are an "authorized" party.

In addition to (or as an alternative to) the use of Non-FBO solicitation, the IRS may choose to set up a "reading room" (or equivalent web site). In such instances, vendors will generally be required to go through a registration process with IRS and complete a Non-Disclosure Agreement (NDA), as conditions for being granted access to the reading room or site. The Contracting Officer and Contracting Officer's Representative (COR) will monitor the full recovery of all returns, return information, or other SBU information disclosed or released to vendors/prospective offerors.

(2) For awarded contracting vehicles— SBU information shall only be released or accessible to those individuals who have been approved, by Personnel Security, for interim or final staff-like access[2] (commensurate with their position sensitivity level), and have a bona-fide "need to know" in Order to perform the work required under the contract for which they have been granted access to such information.

(c) *Fitness and Suitability*. The IRS reserves the right to determine the fitness or suitability of a contractor employee to receive or be assigned staff-like access under a contract, (or continue to have such privileges over the life of the contract) and to have access to SBU information and be permitted to perform (or continue to perform) under the contract if and when it is determined that the contractor employee poses a security risk or otherwise endangers performance.

(d) *Security Screening Precursor*. All contractor employees that require staff-like access to SBU information or information systems in the performance of this contract (regardless of workplace or location), shall be subject to security screening and investigative processing, commensurate with the position sensitivity level, and in accordance with IRM 10.23.2, Contractor Investigations, and Department of the Treasury Security Manual (TD P) 15-71, Chapter II, Section 2. Contractor employees must be favorably adjudicated prior to starting work on the contract or before being granted staff-like access (or interim staff-like access, if approved by PS) to IRS information systems or SBU information.

Pursuant to IR1052.204-9005 – Submission of Security Forms and Related Materials, the contractor shall coordinate security screening and related submissions with Contractor Security Management (CSM) (e.g., the Contradictor Risk Assessment Checklist), as described in P&P

[2] *"Staff-like access,"* refers to unescorted physical or electronic access to IRS owned or controlled facilities, SBU information, or information systems, regardless of location, by contractor employees that have a completed, favorably adjudicated background investigation and whose duration of employee under the contract exceeds 180 days. This access is not unlimited however, and should only be given for the work in which the contract was awarded. *"Interim staff-like access,"* refers to staff-like access privileges that may be granted prior to the completion of the required background investigation. Due to the risk associated with granting staff-like access prior to the completion of the required background investigation, interim staff-like access may only be granted in cases where it has been determined that the risk is acceptable, and approval is granted by IRS, Personnel Security.

No. 39.1(C) – Managing Contractor Employee Access to IRS Owned or Controlled Facilities, Information Systems, or Sensitive But Unclassified (SBU) Information.

(e) *Security Controls and Safeguards*. The contractor shall employ effective technical, operational, and management safeguards or countermeasures to protect the confidentiality, integrity, and availability of SBU information and information systems, consistent with the requirements and objectives of the following statutory and regulatory requirements, and related Treasury or IRS directives, policy and guidance, to include, but not limited to, as applicable—

- E-Government Act of 2002 (P.L. 107-347) Title III, Federal Information Security Act of 2002 (FISMA);
- Privacy Act of 1974 (5 U.S.C. 552A (g)(1), as amended;
- Internal Revenue Code, 26 U.S.C. § 6103;
- 26 C.F.R., § 301.6103(n)-1Disclosure of returns and return information in connection with written contracts or agreements;
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 – Recommended Security Controls for Federal Information Systems and Organizations (as amended);
- Federal Acquisition Regulation (FAR) (to include, but not limited to Part 24 – Protection of Privacy and Freedom of Information and Part 39 – Acquisition of Information Technology);
- Department of the Treasury Security Manual (TD P 15-71);
- Department of Treasury Regulation (DTAR);
- Department of the Treasury Acquisition Procedures (DTAP);
- Internal Revenue Manual (IRM) 10.2.13 – Information Protection;
- IRM 10.8.1 – Information Technology (IT) Security, Policy and Guidance,
- IRM 10.8.2 – IT Security Roles and Responsibilities,
- Publication 4812 – Contractor Security Controls;
- Internal Revenue Service Acquisition Procedure (IRSAP); and
- Applicable FAR clauses or provisions, and local clauses or provisions contained in (or associated with) the IRSAP or IRS Policy and Procedures Memoranda.

Safeguards should be proportional to the sensitivity of the information, and the context in which it is held, and the likelihood and severity of the harm threatened (which, on occasion, may vary in intensity (as will the response) according to the situation or circumstances). Safeguards shall be subject to periodic review and reassessment, and adjustment, as required or warranted, as determined by the IRS.

(f) *General Conditions for Allowed Disclosure*. Any SBU information, in any format, made available to contractor personnel authorized and cleared to receive such information that is marked or that fits the definition and could be marked as SBU information (e.g., using identifying page markers or footers such as OUO or LUO, etc.), shall be used only for the purposes of carrying out the requirements of this contract. SBU information shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary and allowed in the performance of the contract and then only to those who have also received a favorably adjudicated security screening and whose duties or responsibilities require logical and/or physical access to the SBU information in Order to perform under the contract and are authorized by law to have access to the SBU information.

Inspection by or disclosure to anyone other than a duly authorized officer or employee of the contractor shall require prior written approval of the IRS. Requests to make such inspections or disclosures should be addressed to the cognizant Contracting Officer.

(g) *Authority for Disclosure of Returns and Return Information*. As allowed under 26 CFR 301.6103(n)-1 (pursuant to the Internal Revenue Code (26 U.S.C. 6103(n)) and subject to the conditions and limitations set forth therein, for the SBU information category of Returns and Return Information—

(1) Officers and employees of the Treasury Department (and when applicable, a State tax agency, the Social Security Administration, or the Department of Justice) are authorized to disclose returns and return information (as defined in 26 U.S.C. § 6103(b)), for the purposes of tax administration, to any person (i.e., which, for the purposes of this clause, is the contractor), to the extent necessary in connection with a written contract or agreement for the acquisition of—

(i) Equipment or other property; or
(ii) Services relating to the processing, storage, transmission, or reproduction of returns or return information, the programming, maintenance, repair, or testing of equipment or other property, or the providing of other services.

(2) Any person, or officer or employee of the person who receives returns or return information (i.e., the contractor), may—

(i) Further disclose the returns or return information to another officer or employee of the person whose duties or responsibilities require the returns or return information for a purpose described in the preceding paragraph; or

(ii) Further disclose the returns or return information (e.g., to a subcontractor), when authorized in writing by the IRS, to the extent necessary to carry out the purposes described in the preceding paragraphs and as authorized by law. Disclosures may include disclosures to an agent or subcontractor of the person, or officer or employee of the agent or subcontractor.

(3) Pursuant to 26 CFR 301.6103(n)-1 (e) (1)), before a contractor can disclose return or return information to a subcontractor, the subcontractor must agree to permit an inspection by the IRS of its site or facilities, if the agency, at its discretion, makes such a request.

(4) Except as may be provided elsewhere in the contract, the contractor shall neither disclose the identity of the taxpayer (living or deceased) nor any element or aspect of said taxpayer's return or return information, at any time, unless authorized in writing by the IRS –subject to the contractor clearly showing that such disclosure of such information is essential to successful performance of the contract. Requests to disclose the identity of the taxpayer, or any element or aspect of said taxpayer's return or return information shall be addressed to the cognizant Contracting Officer.

(h) *Requests and Demands for Testimony and Production of Documents.* Pursuant to 26 CFR 301.9000-1 through 301.9000-7, IRS officers and employees, as well as contractors, are

required to obtain prior approval before they may produce IRS records or information or testify in judicial or administrative proceedings in response to a demand (subpoena, notice of deposition, court Order, etc.). Delegation Order 11-2 (formerly DO-156. Rev. 17) – Authority to Permit Disclosure of Tax Information and to Permit Testimony or the Production of Documents (IRM 1.2.49.3) sets forth the IRS officials who may authorize testimony or disclosure of IRS records or information in response to certain requests and demands for such information in accordance with applicable disclosure laws (e.g., IRC §6103, IRC §6104, IRC §6105, IRC §6110, IRC §4424, and the Privacy Act).

The contractor shall alert the COR to any requests or demands for IRS information and (in coordination with the COR) seek advice from the IRS Disclosure Office (headquarters or field office, as appropriate) or contact *Ask Disclosure*. The IRS Office of Disclosure, in consultation with and on the advice of IRS Office of Chief Counsel or other functional offices, as appropriate, or as specified in Delegation Order 11-2, will provide guidance –to include, whether the judicial or administrative proceedings will or will not require testimony authorizations, and what additional steps, if any, are necessary. IRM 11.3.35 – Requests and Demands for Testimony and Production of Documents provides additional guidance –to include when no testimony authorization is required in an IRS matter (e.g., when testimony or production of records is requested by Government counsel representing the IRS in an IRS matter).

(i) *Supervision*. All work shall be performed under the supervision of the contractor or the contractor's responsible employees.

The contractor employee may commence work only upon notice of an interim or final approval for staff-like access, notice of revalidation of staff-like access for contractor employee transfers from one IRS contract/Order to another, or when escorted access is approved by an IRS official authorized to grant such access, and the escort will be provided by a qualified escort, as defined in IRM10.23.2 – Contractor Investigations, and is otherwise consistent with IRS security practices and related IRMs, to include, but nor limited to, IRM 1.4.6 – Managers Security Handbook, IRM 10.2.14 – Methods of Providing Protection, and IRM 10.8.1 - Policy and Guidance. As prescribed in IRM 10.23.2, escorting in lieu of staff-like access for IT systems is not allowed.

(j) *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. For the purposes of this clause (and the security and safeguard measures to be employed), the term "subcontractor" (and references to "subcontract") shall include—

- Those in a traditional prime contractor-subcontractor relationship;
- Any person or agent of the prime contractor that has a role in providing services in performance or in direct support of the immediate contract; and
- Any person or third-party service provider that while not necessarily providing services in performance or in direct support of the immediate contract, does otherwise provide services to the prime contract for daily operations or multiple activities that would give that individual(s) insight into or access to IRS information, or IRS or contractor

information systems (at any level) that store or use IRS information (e.g., IT infrastructure support personnel).

Any subcontract (or arrangement or outsourced service) that entails access to SBU information by the subcontractor shall include and flow down the substantially same provisions of this clause. No SBU information or work involving SBU information furnished under this contract shall be released to a subcontractor or subcontracted out without the specific approval of the Contracting Officer (**which, for returns and return information, must be in writing**), and the completion of appropriate background investigations and clearances for all subcontractor employees to be given access to such information.

In addition, **for return and return information**, pursuant to 26 CFR 301.6103(n)-1 (e) (3), the contractor shall make the proposed contract or agreement with the subcontractor available to the IRS before execution of any new contract or agreement. And shall make any existing contract or agreement that incorporates this clause, by modification, available upon request.

(k) *Accounting for SBU Information*. The contractor shall ensure adequate security (that which is necessary to ensure the security objectives of confidentiality, integrity and availability are met) is provided for all IRS information that is collected, processed, transmitted, stored, or disseminated –irrespective of ownership of the information system or infrastructure in use— and that the security is commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information. All SBU information, regardless of form or format, shall be accounted for upon receipt and properly stored before, during, and after use, handling or processing. This shall include accounting for and maintaining inventories on all registers, ledgers, software, programs, online tools, hardware, peripherals, copiers or other "electronic and information technology (EIT)" as defined in FAR Part 2 that are used to (or can) log, store, reposit, record, cache, retain, or preserve SBU information. In addition, all related output, deliverables, or secondary or incidental by-products generated directly or indirectly from the source material shall be given the same level of protection as required for the source material.

(l) *Internal Revenue Code Confidentiality and Penalty Provisions*. Confidentiality requirements for tax returns and return information are established by Section 6103 of the Internal Revenue Code (26 U.S.C. 6103) and the penalties for unauthorized access and disclosure of returns and return information are found in Sections 7213, 7213A and 7431 of the Internal Revenue Code (26 U.S.C. 7213, 7213A and 7431). The willful unauthorized access (commonly referred to as UNAX) or inspection of any taxpayer records including hard copies of returns and return information as well as taxpayer information maintained on a computer is covered by all of these statutes collectively. Unauthorized access or inspection of taxpayer returns and return information (even if the information is not disclosed) is unlawful.

(m) *The Privacy Act*. The general purpose of the Privacy Act of 1974, as amended (5 U.S.C. § 552a) is to balance the Government's need to maintain information about individuals with the rights of the individuals to be protected against unwarranted invasions of their privacy. The Privacy Act establishes special requirements for the Executive Branch of Government when collecting, creating, maintaining, and distributing records that can be retrieved by the name of an individual or other identifier (whether in paper or electronic form). It applies to information on individuals.

(n) *Training*. Contractor employees who require staff-like access to SBU information or information systems to perform their job duties and responsibilities under the contract, regardless of their physical location or workplace, must have received a favorably adjudicated IRS background investigation, and thereafter, shall complete one or more Information Protection briefings (on an annual basis) on computer security, disclosure, privacy, physical security, and/or UNAX, as specified by CSM –commensurate with the assigned risk designations of the position for the work being performed and the category of SBU information to which the employee has access. Individually and collectively, these briefings make up the IRS Security Awareness Training (SAT) requirements for the Service's information assets, as described in IRSAP clause 1052.204-9003 – IRS Security Awareness Training –which must be completed when first assigned, and annually thereafter.

Contractor employees performing in trusted roles that entail *significant responsibility for information security*, as described in NIST SP 800-53 – Recommended Security Controls for Federal Information Systems and Organizations (Revision 3 (AUG 2009)) (*Errata as of May 1, 2010*), NIST Special Publication 800-16 (Rev1), Information Technology Security Training Requirements: A Role- and Performance-Based Model, Treasury Directive Publication (TD P) 85-01 –Treasury Information Technology Security Program (Volume 1), Appendix H, IRM 10.8.1 – Information Technology (IT) Security, Policy and Guidance, and IRM 10.8.2 – IT Security Roles and Responsibilities, (e.g., CIO, CISO, System Administrator, etc.) may be subject to additional, annual requirements for completion of specialized/role-based training, as may be established by IT, Cybersecurity, Security Risk Management.

(o) *Non-Disclosure Agreement (NDA)*. Consistent with TD P 15-71, Chapter II, Section 2, and IRM 10.23.2, each contractor employee who requires access to SBU information shall complete, sign and submit to Personnel Security –through the CO (or COR, if assigned)— an approved NDA. Only contractor employees that have completed NDA and SAT requirements, and have a "bona fide need to know," shall be assigned to and permitted to perform work on contracts/Orders that entail contractor access to SBU information or IRS information systems. Furthermore, the IRS reserves the right to revoke access privilege when the disclosure of the information may compromise the interest of the agency or if the Service determines that such disclosure would identify a confidential informant or seriously impair a civil or criminal tax investigation.

(p) *Encryption*. All SBU information must be protected at rest, in transit, and in exchanges (i.e., internal and external communications). The contractor shall employ encryption concepts to ensure the confidentiality and integrity of the SBU information. Unless more stringent or specific, minimum security requirements are required elsewhere under the contract, the following safeguards and standards, consistent with security controls under NIST SP 800-53 (or IRM 10.8.1 or Publication 4812, as applicable), are indicative of the level and type of encryption safeguards and protective measures to be employed—

- Ensure all disk areas for all computers containing SBU information are encrypted (e.g., by using an Encrypted File System (EFS)).

- Store SBU information on hard disks, but only if contractor-approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance, including upgrades, and are being used.

- Access control to SBU information stored on systems shall include password security, an audit trail, encryption, virus detection, and, as appropriate, information overwriting capabilities.

- Identify an alternate storage site to retain backup media, in the event the information must be recovered. All backup data that contains SBU information must be encrypted.

- All mobile computing devices shall require and have full disk encryption. This includes, but is not limited to, IT resources, including computers, servers, laptop computers, removable Compact Disk (CD) and Digital Video Device (DVD) media, thumb drives, or any media that can be used to house IRS data that can be easily transported by an individual. All data that resides on removable media must be encrypted to comply with Federal Information Processing Standards Publication (FIPS Pub) 140-2 – Security Requirements For Cryptographic Modules.

- Electronic, optical and other removable media shall be kept in a secured area under the immediate protection and control of an authorized employee or locked up. When not in use, the media shall be promptly returned to a proper storage area/container.

- Protect and control information system media during transport outside of controlled areas and restrict the activities associated with transport of such media to employees with an IRS approved interim or final background investigation.

- The contractor must sanitize information, digital, optic, and paper, prior to disposal or release for reuse. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, and CD-ROM), optical disks (DVD) and magnetic-optic (MO) disks must be destroyed by pulverizing, cross-cut shredding or burning. Destruction of media must be conducted only by trained authorized personnel. A log must be maintained to provide a record of media destroyed. The log must include, at a minimum, (i) the date of destruction; (ii) content of media; (iii) identifying serial number or other tracking number, if applicable; (iv) type of media (CD, cartridge, etc.); (v) media destruction performed; (vi) personnel performing the destruction; (vii) and witness(es) to the destruction.

- When SBU information is transmitted across internal and external networks, cryptography (symmetrical or asymmetrical key encryption) should be employed (unless otherwise protected by alternative physical measures (e.g., protected distribution systems)), or in the case where the contractor is relying on a commercial service provider for transmission services as a commodity rather than a fully dedicated service, the contractor shall employ appropriate compensating security controls. The information system must perform all cryptographic operations using FIPS Pub 140-2 validated cryptographic modules with approved modes of operation. A list of NIST validated modules is available at the following link: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#765.

- When exchanging SBU information through email or network protocols, encryption shall be used. For routine email with IRS, contractors with access to IRS systems shall apply for access privileges to and use Secure Registration Based Email (SRBE); and contractors

without access to SRBE shall use an approved application for digitally encrypting e-mail messages and attachments for transmission. File compression products must be FIP140-2 compliant (e.g., SecureZip). For those contracts that routinely require bulk computer-to-computer file transfers, the contractor shall coordinate with the COR and the IT, Enterprise Operations, Enterprise Computing Center, Mainframe Operations Branch, File Transfer Section on a Secure Data Transfer (SDT) solution.

- The physical environment and the security of that environment must also be addressed to ensure adequate protection of both paper based SBU information and SBU information in electronic form. Whenever possible, computer operations must be in a secure area with restricted access. In situations such as home work sites, remote terminals, or office work sites where all of the requirements of a secure area with restricted access cannot be maintained, the equipment shall receive the highest level of protection that is practical. Minimum physical security requirements must be met, such as keeping SBU information locked up when not in use. Removable media also must be encrypted and labeled SBU information when it contains such information.

(q) *Use of Personally-Owned and Other Non-Government Furnished Equipment.* In accordance with IRM 10.8.1.5.2.8 – Personally-Owned and Other Non-Government Furnished Equipment, non-Government furnished IT equipment includes personally owned and contractor-owned IT equipment (e.g., laptops, PDAs, workstations, digital media, monitors, servers, routers, firewalls).; and personally owned equipment shall include all individually owned systems, devices, software, and media (e.g., thumb drive, CD, removable hard drive).

Information that has been determined to have a *potential impact* –on organizations or individuals— rating of **High** for any security objective (confidentiality, integrity, or availability), as described in FIPS 199 – Standards for Security Categorization of Federal Information and Information Systems, shall not be stored, processed, accessed, or transmitted using personally-owned equipment.

Personally owned equipment shall not be used to process, access, or store sensitive/classified information, nor shall it be connected to IRS systems and networks directly or via Virtual Private Network (VPN).

Contractors and vendors of the IRS using contractor-furnished IT equipment shall ensure the equipment meets the minimum security requirements detailed in the IRS contract/statement of work. Refer to the Contractors and Outsourced Operations section of IRM 10.8.1 and IRM 10.8.2 for additional detailed information.

Government-furnished equipment (e.g., thumb drives, laptop, printer) shall not be connected to non-Government furnished equipment.

Approvals by the Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO) and Authorizing Official (AO) are required for connection of personally-owned or contractor-owned IT devices to IRS systems or networks.

Refer to IRM 10.8.1.5.2.8 for additional guidance on use or exceptions on use of Personally-Owned and Other Non-Government Furnished Equipment. and IRM 10.8.26 – Laptop Computer Security Policy for guidance on minimum security controls to safeguard laptops.

(r) *Special Handling or Delivery of SBU information or Work Products Containing SBU Information*. Reserved.

(s) *Notification Requirement on Prohibitions and Penalties for Unauthorized Disclosure or Misappropriation of SBU Information (in general), Unauthorized Inspection or Disclosure Specifically for Returns and Return Information, and Improper Disclosure of Information Subject to the Privacy Act.*

(1) Each officer or employee of the contractor or subcontractor at any tier to whom SBU information may be made available or disclosed shall be notified in writing by the contractor that SBU 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 SBU information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. Sections 641 and 3571. Section 641 of 18 U.S.C. provides, in pertinent part, that whoever knowingly converts to his use or the use of another, or without authority sells, conveys, or disposes of any record of the United States or whoever receives the same with the intent to convert it to his use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine or imprisoned up to ten years or both.

(2) Each officer or employee of any person (contractor or subcontractor) at any tier to whom returns or return information is or may be disclosed shall be notified in writing by the person (contractor or subcontractor) that returns or return information in any format 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 (contractor or subcontractor) 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, and, 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.

(3) Each officer or employee of any person (contractor or subcontractor) 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 (contractor or subcontractor) 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.

(4) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(I)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established 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.

Note: Contractors must make employees aware that disclosure restrictions and penalties apply even after the contract is completed, as well as after employment with the contractor has ended.

(t) *Incident* [3] *and Situation Reporting.* Contractor employees should be advised to contact their manager, supervisor or contractor-designated person or office **within the first hour** that it becomes known, that an information system or SBU information has been compromised (e.g., inspected or disclosed without authorization or disclosed to an unauthorized party, loss or stolen, misdirected, intercepted, hacked, etc.) or other situation has taken place that poses an imminent threat (or resulted in actual harm) to persons or property. **Within the first hour, the contractor shall report the incident/situation to the COR** (or the CO or other backup when the COR is unavailable). A key aspect of incident management is the timely reporting of significant conditions or situations. Prompt reporting is essential in Order to advise all levels of management of conditions that affect the operation of the Service as well as to allow analysis of current information. **Concurrent with its reporting it to the COR, the contractor shall report incidents/situations as follows** 24x7x365—

- All physical security incidents or situations that pose an imminent danger or threat to persons or property (e.g., situations that may require evaluation, containment or shelter-in-place, or medical attention) should be reported to the Situation Awareness Management Center (SAMC) through any of the following methods:
  - Telephone: (202) 283-4809 (local) or toll free hotline at (866) 216-4809
  - Fax: (202) 283-0345
  - E-mail: samc@cirsc.irs.gov ,

[3] An "incident," as defined by NIST Special Publication 800-61, Computer Security Incident Handling Guide, Revision 1, March 2008, "is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." Adverse events may include the loss of data *confidentiality*, disruption of data or system *integrity*, disruption or denial of *availability*, loss of accountability, or damage to any part of the system.

As appropriate, also contact local emergency personnel or authorities (e.g., police, fire department, EMT, or on-site personnel with related training or responsibilities).

- All cyber security incidents or losses of CIA shall be reported to the Computer Security Incident Response Center (CSIRC) through any of the following methods:
  - Telephone: (202) 283-4809 (local) or toll free hotline at 866-216-4809 (or (or TTY access (Federal Relay Services) 1-800-877-8339)
  - Fax: (202) 283-0345
  - Online: https://www.csirc.web.irs.gov/incident/
  - E-mail: csirc@csirc.irs.gov

  Information about unclassified cyber security incidents of a sensitive nature shall be transmitted using secure messaging or alternative forms of encryption.

- 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.

The contractor shall also take action to minimize damage or neutralize the potential for further compromise, and thereafter take appropriate, prudent steps to prevent recurrence, or protect the safety of others.

(u) *Administrative Remedies*. Unauthorized inspection(s) or disclosure(s) of SBU by the contractor or its employees, agents or subcontractors, may be considered a breach of the contract. In the event such incidents occur, or when it is determined the contractor has failed to satisfy the safeguard or privacy provisions of the contract and immediate remedial or corrective action cannot be taken by the contractor (or the remedial or corrective action is inadequate or ineffectual), the Contracting Officer may suspend further disclosures of SBU information, invoke the Default clause of the contract (e.g., FAR clause 52.249-8 - Default (Fixed-Price Supply and Service)), incorporated into the contract by reference, or if a termination for default or cause is not in the best interest or the Government, may elect to pursue a termination for convenience (under the clause of that class incorporated into the contract by reference), or employ other administrative remedies available to the Government.

(v) *Dispositioning SBU Information*. As a general rule, it is contrary to the Internal Revenue Code and the general operating policies of the IRS to allow a contractor to retain returns or return information or other categories of SBU information, or federal records released to the contractor in performance of the contract (or created as a result of the contract), after the purposes of (or objectives and service requirements under) the contract have been satisfied, or its term complete.

All SBU information processed during the performance of this contract, or to which the contractor 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,[4] shall be completely purged

[4] In accordance with IRM 1.15.1.1, ". . . under the statutory definition of 'Federal Records.' Records are considered media (or format) neutral. Consequently, procedures for records and information management apply to official

from all data storage components of the contractor's facility(s) and computer systems, and no SBU information will be retained by the contractor either—

(i) when it has served its useful, contractual purpose, and is no longer needed to meet the contractors contractual obligations to the IRS,
(ii) at the time the IRS work is completed or when the contract expires (whichever comes first), or
(iii) if and when the contract is terminated (for convenience, default, or cause).

Similarly, any mobile computing devices, EIT equipment and devices, removable storage devices, and optical storage devices shall be purged of SBU information, and any [partial or complete] hard copy printouts, duplications or transcriptions of SBU information shall be given to the IRS Contracting Officer or his/her designee (e.g., COR), or destroyed, as provided in the contract or instructed by the Contracting Officer.

The contractor shall maintain records on the methods, times and places of disposal or destruction of SBU information.

Typically, exemptions to retain information/data/records beyond the term of the contract are limited to situations in which certain data elements can not be immediately and completely expunged as a result of technical difficulties.
(*Note: Exemptions would not include conditions such as a contractor's needs to retain information/data/records in Order to comply with industry protocols or standards, or state licensing or practitioner requirements.)*

If immediate purging of all data storage components is not possible, the contractor shall make application to the Contracting Officer to retain the SBU information for an additional period and provide the following (for the initial and any subsequent applications)—

(i) The basis for why the SBU information cannot (or should not) be purged at the conclusion of the contract and needs to be retained for the projected retention period (which, for approval purposes, is typically limited to technical difficulties experienced or anticipated with immediate expunging/dispositioning);
(ii) Written assurances to the Contracting Officer that any SBU information remaining in any storage component will be safeguarded to prevent unauthorized inspection or disclosure, and the protective measures that will be implemented to safeguard SBU information (e.g., locked containers, encrypted files, limited role-based access, etc);
(iii) A projected retention period or timeline on how long the information may need to be retained; and
(iv) If and when requested, any additional information the IRS may need to make its determination to allow (or not allow) the contactor to retain the SBU information at issue.

The Contracting Officer, in consultation and coordination with the end user (originating office)/Business Operating Division, Privacy, Disclosure and appropriate Service components with security related functions or responsibilities, will advise the contractor of the agency's

---

IRS recorded information in all format types. See Title 44 U.S.C. §2901(2) for a definition of 'Records Management,' and §3301 for a definition of 'Federal Records.'"

decision. Approval to retain SBU information beyond the period when it should normally have been returned, purged, destroyed, or otherwise disposed or dispositioned, as instructed, shall be at the sole discretion of the IRS. Approval, if given, may be affected by the parties, as determined appropriate, under the existing contracting vehicle, or by entering into a separate, written Memorandum of Understanding or Agreement that will establish the period of the hold/retention (forbearance on the immediate return of SBU information), and the terms and conditions of such an agreement (to include elements presumably similar to those in the subject contract with respect to safeguarding SBU information, and the criminal or civil sanctions the vendor may be subject to for unauthorized disclosure or inspection of the held/retained SBU information, or for its loss, theft, or alteration without proper IRS authorization).

Even in those rare instances when an exemption is allowed, the Service's limits of patience in the time and effort necessary for expunging (or otherwise properly disposing of) its data/information should not be tested, and its insistence on full, complete and timely compliance is not subject to negotiation.

Failure to return all SBU information to the IRS–to include derivative works produced in performance of the contract—or provide verification, to the satisfaction of the IRS, of the comprehensive removal of SBU information and successful purging of said SBU information from the contractor's information systems and equipment (at either the end of the contract or any subsequent period allowed for) as requested or demanded by the Government, may subject the contractor to the full extent of rights and remedies available to the Government under the contract still in effect, or if appropriate, penalties or punishments provided by law. For example, the Contracting Office may explore withholding or delaying final payment, as may be allowed under payment-related contract clauses, as one administrative remedy to ensure compliance; or as appropriate, rate past performance assessments to reflect any failure to comply; or, when justified, pursue criminal or civil penalties provided by law for unauthorized inspection or disclosure of SBU information or violations of Privacy Act protections or requirements for handling federal records.

(w) *Other Safeguards*. [*Insert any additional disclosure safeguards provided by the requisitioner or that the Contracting Officer determines are necessary and in the best interest of the Government and not addressed elsewhere in the contract*.]

(End of Clause)

IR1052.239-9014 Information Systems and Information Security Controls for Contracting Actions Subject to Internal Revenue Manual (IRM) 10.8.1 (Jun 2013)

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.* (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 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 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.

(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.

(End of clause)

IR1052.239-9015 Information Systems and Information Security Controls for Contracting Actions Subject to Publication 4812 (Jun 2013)

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.

(c) *Publication (PUB) 4812 Applicability.* This contracting action is subject to Publication 4812 – Contractor Security Controls. PUB 4812 is available at: http://www.irs.gov/uac/Procurement.

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 that have a total value (inclusive of any options) greater than the micro-purchase threshold (for services), and in which contractors and contractor employees (or subcontractors (and 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 .

(d) *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.

(e) *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.

(End of clause)

IR1052.239-9016 Information System and Information Security Control Standards and Guidelines Applicability (Jun 2013)

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

While IRM 10.8.1 and PUB 4812 are both based on NIST SP 800-53 (Rev. 3), 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 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 Contracting Officer.*)

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 Contracting Officer, in consultation with IT Cybersecurity, determines otherwise.

e. If required by the 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.

(End of clause)