SECTION IV: CONTRACT CLAUSES (FAR, DTAR, IRSAP)

All clauses provided by GSA's Professional Services Schedule (PSS), Financial and Business Solutions (FABS), Category 520 -4 Debt Collection apply to this acquisition.

In addition, the following clauses and provisions apply:

1. DISCLOSURE CLAUSES

1.1 IRSAP 1052.224 -9000(a) - DISCLOSURE OF INFORMATION —SAFEGUARDS (JAN 1998)

In performing the services described herein, the Contractor agrees to comply and assume responsibility for compliance by his/her employees with the following requirements:

(a) All work shall be performed under the supervision of the Contractor or the Contractor's responsible employees.

(b) Any confidential tax information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Confidential tax information includes all identifying taxpayer informa tion and return or return information as defined by section 6103(b) of the Internal Revenue Code. This confidential tax information shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contr act. Inspection by or disclosure to anyone other than an officer or employee of the Contractor shall require prior written approval of the Internal Revenue Service. Requests to make such inspections or disclosures should be addressed to the IRS Contracti ng Officer.

(c) All confidential tax information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output shall be given the same level of protection as required for the source materi al.

(d) The Contractor certifies that the data processed during the performance of this contract shall be completely purged from all data storage components of his/her computer facility, and no output will be retained by the Contractor at the time the I RS work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized inspections or disclosures.

(e) Any spo ilage or any intermediate hard copy printout, which may result during the processing of IRS data, shall be given to the IRS Contracting Officer or his/her designee. When this is not possible, the Contractor will be responsible for the destruction of the s poilage or any intermediate hard copy printouts, and shall provide the IRS Contracting Officer or his/her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

(f) No work involving informat ion furnished under this contract will be subcontracted without the specific written approval of the IRS Contracting Officer. Subcontractors are held to the same level of confidentiality and privacy requirements inclusive of special contract requirements as is the Contractor.

(g) All computer systems processing, storing and transmitting tax data must meet or exceed controlled access protections (CAP) wherein the operating security features of the system

has the following minimum requirements: an approved security policy, accountability, assurance and documentation. All security features must be available (object reuse, audit trails, identification/authentication and discretionary access control) and activated to protect against unauthorized access, use, disclosure, disruption, modification, or destruction of federal tax information. All computer systems are required to be compliant with the Federal Information Security Management Act of 2002 (FISMA) pursuant to Section 3544(a)(1)(A)(ii). In this regard, NIST standards and guidance must be implemented and adhered to by the Contractor.

(h) Should a Contractor or one of his/her officer(s) or employees make any unauthorized inspection(s) or disclosure(s) of confidential tax information, the terms of the de fault clause (FAR 52.249-8), incorporated herein by reference, may be invoked, and the Contractor will be considered to be in breach of this contract.

(i) The Contractor will ensure that his/her officers and employees will adhere to the written procedures from IRS in regards to the receipt, processing and handling of all tax returns and return information, as well as the storage and transmitting thereof. The location of all tax returns and return information and any products made there from, will be fully accounted for (logged/tracked) at all times by the Contractor .

(j) Reporting Requirements: The Contractor will submit a Safeguards Procedures Report to the IRS COR 45 days prior to initial receipt of Federal tax information. The COR will refer to the report to the Office of Safeguards for approval, prior to actual disclosures of Federal tax information. The Contractor will annually thereafter, submit a Safeguards Activity Report to the IRS COR. See Section III.9 Schedule of deliverables.

1.2 IRSAP 1052.224-9000(d) - DISCLOSURE OF "OFFICIAL USE ONLY" INFORMATION SAFEGUARDS (JAN 1998)

Any Treasury Department information made available or to which a ccess is provided, and which is marked or should be marked "Official Use Only", shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any person except as may be necessar y in the performance of the contract. Disclosure to anyone other than an officer or employee of the Contractor shall require prior written approval of the IRS. Requests to make such disclosure should be addressed to the IRS Contracting Officer.

1.3 IRSAP 1052.224-9001(a) - DISCLOSURE OF INFORMATION --CRIMINAL/CIVIL SANCTIONS (JAN 1998)

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

(b) 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 exten t not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person (Contractor or subcontractor) shall al so 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 for each act of unauthorized inspection with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection plus in the case of a willful inspection or an inspection which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRC Sections 7213A and 7431.

(c) Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for unau thorized disclosure imposed by the Privacy Act of 1974, 5 USC 552a. Specifically, 5 USC 552a(i)(1), which is made applicable to Contractors by 5 USC 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 hereunder, and who knowing that disclosure of the spec ific 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.

1.4 IRSAP 1052.224 -9001(b) - DISCLOSURE OF INFORMATION —OFFICIAL USE ONLY (JAN 1998)

Each officer or employee of the Contractor to whom "Official Use Only" information may be made available or disclosed shall be notified in writing by the Contractor that "Official Use Only" 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 "Official Use Only" information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 USC Sections 641 and 3571. Section 641 of 18 USC 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 has been converted, shall be guilty of a crime punishable by a fine or imprisoned up to ten years or both.

1.5 IRSAP 1052.224 -9002 - DISCLOSURE OF INFORMATION – INSPE CTION (JAN 1998)

The Intern al Revenue Service or designee shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the facilities and operations provided for the performance of an y work under this contract. On the basis of such inspection, the Contracting Officer may require specific measures in cases where the Contractor is found to be noncompliant with contract confidentiality and privacy safeguard requirements.

1.6 IR 1052. 224-9009 – IRS INFORMATION PROTECTION AND 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 al l employees (including contractor and subcontractor) involved in the management, use, or operation of Federal information and information systems. In addition, contractors (including subcontractor) and their employees are subject to the Taxpayer Browsing P rotection Act of 1997, which prohibits willful unauthorized inspection of returns and return information. Violation of the Act could result in civil and criminal penalties.

(a) The contractor must ensure all contractor (including subcontractor) personnel complete one or more Information Protection briefings on computer security, disclosure, privacy, physical security, and/or unauthorized access to taxpayer accounts (UNAX), as specified by Contractor Security Management (CSM). CSM can be reached at awss.cs m.training@irs.gov. Individually and collectively, these briefings make up the IRS Security Awareness Training (SAT) requirements for the Service's information assets. **Exception:** Contractor personnel (including subcontractors) performing under IRS contract s with Nonprofit Agencies Employing People Who Are Blind or Severely Disabled (as described in FAR Subpart 8.7) are exempted from the aforementioned SAT requirements, unless the contractor requests SAT, or there is a compelling justification for requiring the training that is approved by the Contracting Officer (CO), in consultation with CSM. An example of this would be in an instance where a visually impaired employee is assigned to perform systems development and has potential staff -like access to IRS inf ormation.

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

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

(ii) Access to SBU Information and IT Systems SAT
Contractor personnel, including subcontractor personnel, required to co mplete SAT include, but are not necessarily limited to, those involved in any of the following activities:

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

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

- Medical;

- Cafeteria;
- Landscaping;
- Janitorial and cleaning (daylight operations);
- Building maintenance; or
- Other maintenance a nd 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 facili ties 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. Faci lities performing pipeline processing and/or have an exemption to the clean desk policy are:

Clean Desk Waiver Facilities	
Facilities	Address
KY2032	333 Scott St., Covington, KY 41001
KY3005	300 Madison Ave., Covington, KY
MI1951	985 Michigan Ave., Detroit, MI 48226
MN1600	30 East Seventh St., St. Paul, MN
TX2225	2191 Woodward St., Austin, TX 78744

Pipeline Processing Facilities:	
Facilities	Address
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
KY3016	7125 Industrial Rd., Florence, KY 41042
MO1937	Kansas City Campus, 33 W. Pershing Rd., Kansas City, MO
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 12^{tn} St., Ogden, UT 84201

(Note: The facilities listed above can change annually and are only authorized for one year.)

(v) Training Certificate/Notice

The contractor must submit confirmation of completed SAT by either:

A) Using form 14616 located at:
http://core.publish.no.irs.gov/forms/internal/pdf/66610g14.pdf for those who take training other than online; or

B) Certifying online at the Mandatory Briefing website awss.csm.training@irs.gov, with a copy to the CO and Contracting Officer's Representati ve (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 cont rols being used to protect information,

including confirmation of security awareness training.

(vi) Annual Training

For contracts/orders/agreement exceeding one year in length, either on a multiyear or on multiple year basis, contractor must ensure that personnel complete SAT annually no later than October 31st of the current calendar year. The contractor must submit confirmation of completed annual SAT on all personnel assigned to this contract/order/agreement, via email, to the CO, COR, and CSM upon co mpletion, but no later than November 15th of the current calendar year or as requested by CSM (whichever date is earlier).

(b) SAT is available on the Mandatory Briefing web site http://e - learning.web.irs.gov/Briefings/Contractors/contractor.html; or if this site is not accessible, SAT materials will be made available by CSM at awss.csm.training@irs.gov.

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

(End of Clause)

1.7 IR1052.224 -9008 – SAFEGUARDS AGAINST UNAUTHORIZED DISCLOSURE OF SENSITIVE BUT UNCLASSIFIED INFORMA TION (NOV 2015)

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

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

2. Confidentiality requirements for tax returns and return information are established by Section 6103 of the Inter nal Revenue Code (26 USC 6103), and the penalties for unauthorized access and disclosure of returns and return information are found in Sections 7213, 7213A and 7431 of the Internal Revenue Code (26 USC 7213,7213A and 7431).

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

4. As directed by the Contracting Officer, the contractor will be required to input data into Archer or a similar system to describe the security controls being used to protect information.

5. Eligibility, Fitness and Suitability. Contractor (including subcontractor) personnel hired for work within the United States or its terr itories and possessions and who require access, wherever the location, to IRS owned or controlled facilities or work on contracts that involve the design, operation, repair, or maintenance of information systems, and/or require access to SBU information, m ust meet the eligibility requirements under IRM 10.23.2, Personnel Security, Contractor Investigations, and shall be subject to security screening and investigative processing, commensurate with the position sensitivity level, and in accordance with IRM 10 .23.2, and TD P 15-71. Contractor (including subcontractor) employees must be favorably adjudicated prior to starting work on the contract/order or before being granted staff -like access (or interim staff -like access, if approved by Personnel Security) to IRS information systems or SBU information.

6. General Conditions for Allowed Disclosure. Any SBU information, in any format, made available to contractor (including subcontract) personnel shall be treated as confidential information and shall be used on ly for the purposes of carrying out the requirements of this contract. Inspection by or disclosure to anyone other than a duly authorized officer or employee of the contractor (including subcontractor) shall require prior written approval of the IRS. Reque sts to make such inspections or disclosures shall be addressed to the Contracting Officer (CO).

7. Nondisclosure Agreement. Consistent with TD P 15 -71, Chapter II, Section 2, and IRM 10.23.2.17 - Nondisclosure Agreement for Sensitive but Unclassified Inf ormation, each contractor (including subcontractor) employee who requires access to SBU information shall complete, sign and submit to Personnel Security – through the CO (or COR, if assigned) — an approved Nondisclosure Agreement prior to being granted ac cess to SBU information under any IRS contract or order.

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

9. Incident and Situation Reporting. The contractor (including subcontractor) shall report any incident/situation in accordance with I RM 10.8.1.4.8.5 - Incident Reporting and to the COR. Concurrent with its reporting it to the COR, the contractor (including subcontractor) shall report incidents/situations (24x7x365) to Computer Security Incident Response Center (CSIRC)(IT infrastructure) /Situation Awareness Management Center (SAMC) (anything that does not affect the IT infrastructure) through any of the following methods:

Telephone: (202) 283 -4809 (local) or toll free hotline at (866) 216 -4809
Fax: (202) 283 -0345
Email: samc@cirsc.irs .gov

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

10. Access to Processing and Storage of Sensitive but Unclassified (SBU) Information. The contractor (including subcontractor) shall not allow contractor or subcontractor employees to access, process or st ore SBU on Information Technology (IT) systems or assets located outside the continental United States and its outlying territories. Contractors (including subcontractors) utilizing their own IT systems or assets to receive or handle IRS SBU data shall not commingle IRS and non IRS data.

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

•When it has served its useful, contractual purpose, and is no longer needed to m eet the contractor's (including subcontractor) other, continuing contractual obligations to the IRS or

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

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

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

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

13. Other Safeguards. None identified.

(End of Clause)

2. INFORMATION TECHNOLOGY (IT) ACCESS AND SECURITY CLAUSES

2.1 IR1052.239 -9007 – ACCESS, USE OR OPERATION OF IRS INFORMATION TECHNOLOGY (IT) SYSTEMS BY CONTRACTORS (APR 2015)

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 (including subcontractor) employees authorized staff -like (unescorted) access to Trea sury/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 (SBU) information sha ll comply with the IRS Information Technology Security Policy and Guidance, Internal Revenue Manual (IRM) 10.8.1, 10.8.2, and IRS Publication 4812. Copies of IRM 10.8.1 and 10.8.2 are available at http://www.irs.gov/irm/. This requirement applies to contra ctors who are using contractor/subcontractor -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/pub/irs -procu re/Publication -4812---Contractor --Security -Controls.pdf .

2. Access Request and Authorization. Within ten (10) business days after contract award or issuance of an order, the contractor shall provide the Contracting Officer' s Representative (COR) and the Contractor Security Management (CSM), via email to awss.csm.training@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 req uested. 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.

Contractor (in cluding subcontractor) employees 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 IRM 10.23.2 and is otherwise consistent with IRS security practices and relat ed 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. Upon notification of a favorable adjudication of a security screening, the COR will comple te an Online 5081 (OL 5081), Automated Information System 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 understan ds 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 requir ements 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, immedia te 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. Contractor (including subcontractor) employees, like Federal employees, have no inhere nt right to use Government IT resources and this policy does not create the right to use Government IT resources for nongovernmental purposes. See IRM 10.8.27, Exhibit 10.8.27 -1, Prohibited Uses of Government IT Resources, for specific examples of prohibit ed uses. See Title 5 - Code of Federal Regulations (CFR) - Part 734 – Political Activities of Federal Employees, for specific examples of prohibited political activities.

b. The contractor (including subcontractor) shall report any incident/situation in accordance with IRM 10.8.1.4.8.5 - Incident Reporting and to the Contracting Officer and COR. Concurrent with its reporting it to the COR, the contractor shall report incidents/situations (24x7x365) to Computer Security Incident Response Center (CSIRC)(IT infrastructure)/Situation Awareness Management Center (SAMC) (anything that does not affect the IT infrastructure) through any of the following methods:

Telephone: (202) 283-4809 (local) or toll free hotline at (866) 216-4809/
TTY at 800-877-8339
Fax: (202) 283-0345
Email: samc@cirsc.irs.gov

- 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 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 email.

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)

2.2 IR1052.239-9014 – INFORMATION SYSTEMS AND INFORMATION SECURITY CONTROLS FOR CONTRACTING ACTIONS SUBJECT TO INTERNAL REVENUE MANUAL (IRM) 10.8.1 (APR 2015)

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

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

(b) *IRM 10.8.1 Applicability.* This contract action is subject to Internal Revenue Manual (IRM) Part

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

(c) Based on Title III of the E -Government Act of 2002 (Public Law 107 -347), also known as the Federal Information Security Management Act of 2002 (FISMA), and standards and guidelines developed by the National Institute of Standards and Technology (NIST), IRM 10.8.1 provides overall IT security control guidance for the IRS, and uniform policies and guidance to be used by each office, or business, operating, and functional unit within the IRS that uses IRS information systems to accomplish the IRS mission.

(d) *Contractor Security Representative.* The contractor shall assign and identify, in its offer, a Contractor Security Representative (CSR) and alternate CSR to all contracts requiring access t o 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 informati on systems in accordance with the terms and conditions of the contract and all applicable security controls. If required by the Contracting Officer's Representative, the contractor will be required to input data into a system, to be defined by the IRS, to describe the security controls being used to protect information.

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

(End of clause)

2.3 IR1052.239 -9015 – INFORMATION SYSTEMS AND INFORMATION SECURITY CONTROLS FOR CONTRACTING ACTIONS SUBJECT TO PUBLICATION 4812 (APR 2015)

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) a re 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 adher e 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 availabl e at:
http://www.irs.gov/pub/irs -procure/Publication -4812---Contractor --Security-Controls.pdf.
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 (Pub lic 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 man agement (TOM) security controls and standards required of under contracts for services in which contractor (or subcontractor) employees will either—

- Have access to, develop, operate, or maintain IRS information or information systems on behalf of the I RS (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 sub contractor 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 ma nual 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 r eviews – 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, facil ities, 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 th e 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 an y 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)

2.4 IR1052.239-9016 – INFORMATION SYSTEM AND INFORMATION SECURITY CONTROL STANDARDS AND GUIDELINES APPLICABILITY (APR 2015)

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

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

o Publication 4812 – Contractor Security Controls dated July 2014.

While IRM 10.8.1 and PUB 4812 are both based on NIST SP 800-53 (Rev. 4), they apply to different operating environments —internal and external to the organization, respectively. The contractor, by signing its offer, hereby asserts to the best of its knowledge and belief that the security control guideline(s) most suitable and applicable to the immediate contracting action, with due consideration to its proposed approach (and work environment) for fulfilling the Government's requirements and standards for applicability described herein, is as follows (*check only one block*):

____IRM 10.8.1 only ____PUB 4812 only ___Both IRM 10.8.1 and PUB 4812

Unless the Contracting Officer (CO) determines, in consultation with Cybersecurity, that a different (or a second) security control standard or guideline is warranted, the security level selected/applied for by the contractor under IR1052.239-9016 shall stand. In the event the Government determines a different (or second) security control standard or guideline is warranted, the CO shall advise the contractor, in writing, of the Government determination, and reflect the correct/appropriate security control standard or guideline in the ensuing contract.

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

_____ _____ Core (C) Security Controls (Abbreviated "C")

_____ _____ Core (C) plus value greater than Simplified Acquisition Threshold (SAT) (Abbreviated "CSAT")

_____ _____ Core (C) plus Networked Information Technology Infrastructure (NET) (Abbreviated "CNET")

_____ _____ Core (C) plus Software Application Development/Maintenance (SOFT) (Abbreviated "CSOFT")

(*See PUB 4812, Appendix C for guidance in selecting the security control level most suitable and appropriate to the immediate contracting action. If additional guidance is needed in selecting the security control level, contact the CO.*)

b. The contractor, by signing its offer, hereby asserts to the best of its knowledge and belief that the security control level under PUB 4812 most suitable and applicable to the imme diate 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 det ermines, 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 pro vide a plan and document the implementation of this plan to ensure that all hard copy and electronic data is returned to the IRS, sanitized, or destroyed.

d. Failure by the contractor to check any block will result in the use of both guidelines (and for the PUB 4812 portion, use of the most stringent security control level (CSOFT)) until and unless the CO, in consultation with IT Cybersecurity, determines otherwise.

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

(End of clause)

2.5 IR1052.204 -9007 – IRS SPECIALIZED INFORMATION TECHNOLOGY (IT) SECURITY TRAINING (ROLE -BASED) REQUIREMENTS (APR 2015)

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

(b) Identifying Candidates with a Sign ificant Role or Responsibility for Information/IT Security.

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

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

(3) In collaboration with the Enterprise FISMA Services (EFS) Group in IT Cybersecurity, Security Risk Management and AWSS , Physical Security, Contractor Security Management , the COR will

review the list and confirm that the employee(s) will serve in roles that entail significant responsibility for information/IT security, and will determine that the received training is adeq uate. The COR will inform the Contractor of the determinations. Indicators of who should complete specialized role -based training annually include, but are not limited to —

• Percentage of duties devoted to information/IT security. Typically, those with 50% of their work related to FISMA duties.
• Characteristics. Those privileged network user accounts that allow individual full system permissions to the resources within their authority or to delegate that authority.
• Catalog of Roles. Those serving in roles identified in the "Required Training Hours for IRS Roles" document maintained at the IT, Cybersecurity, Security Risk Management intranet site for Specialized IT Security Training.

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

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

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

(f) Training Certificate/Notice: The contractor shall submit confirmation of annu ally completed specialized IT security training (role -based) using the Government system identified by AWSS, PSEP, Contractor Security Management for each employee identified, with a copy to the Contracting Officer and COR, upon completion of the training.

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

3. PERSONNEL SECURITY AND BACKGROUND INVESTIGATION CLAUSES

3.1 IR1052.204 -9005 – SUBMISSION OF SECURITY FORMS AND RELATED MATERIALS (OCT 2015)

As described in Department of the Treasury Security Manual (TD P 15 -71), Chapter I, Section 1, Position Sensitivity and Risk Designation, Contractor personnel assigned to perform work under an IRS contract/order/agreement must undergo security investigative processing appropriate to the position sensitivity and risk level designation associated to determine whether the Contractor (including subcontractor) personnel should be permitted to work in the identified position. The Contracting Officer's Representative (COR) (in the absence of the COR, the Contracting Officer (CO)) shall work with the contractor to ensure that contractor (or subcontractor) employee is granted staff-like access to Sensitive but Unclassified (SBU) information, IRS/contractor (including subcontractor) facilities, information system/asset that process/store SBU information

without the required investigation.

For security requirements at contractor faci lities using contractor -managed resources, please reference Publication 4812, Contractor Security Controls. The contractor shall grant staff -like access to IRS SBU information or information system/assets only to individuals who have received staff-like access approval (interim or final) from IRS Personnel Security.
a. Contractor (including subcontractor) personnel performing under an agreement that authorizes staff-like access to and in IRS/contractor (including subcontractor) facilities, and access to SB U information or information systems are subject to (and must receive a favorable adjudication or affirmative results with respect to) the following eligibility/ *suitability* pre-screening criteria, as applicable:
(1) IRS account history for tax compliance (for initial eligibility, as well as periodic checks for continued compliance while actively working on IRS contracts);
(2) Selective Service registration compliance;
(3) U.S. citizenship/lawful permanent residency compliance;
(4) Background investigati on forms;
(5) Credit history;
(6) Federal Bureau of Investigation fingerprint results; and
(7) Prior federal government background investigations.

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

____IRS provided Risk Assessment Checklist (RAC) Form 14606;

____Non-Disclosure Agreement (if contract terms grant SBU access); and,

____Any additional required security forms, which will be made available through CSM and the COR.

b. Tax Compliance, Credit Checks and Fingerprinting:

1. Contractors (including s ubcontractors) whose duration of employment exceeds 180 days must meet the eligibility/suitability requirements for access and shall undergo a background investigation based on the assigned position risk designation as a condition of work under the Governm ent contract/order/agreement.

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

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