Publication 4812

Contractor Security Controls

Handling and Protecting Information or Information Systems

****This Publication Pertains to IT Assets Owned and Managed at Contractor Sites****

Publicationn 4812 (Rev. 10-2015) Catalog Number 54170T Department of the Treasury **Internal Revenue Service** www.irs.gov

Highlights of Publication 4812

Publication 4812 is designed to identify security requirements for contractors and any subcontractors supporting the primary contract. It identifies security controls and requirements for contractors (and their subcontractors) who handle or manage Internal Revenue Service (IRS) Sensitive But Unclassified (SBU) information on or from their own information systems or resources. The level of required security controls may vary depending on the duration, size, and complexity of the contract.

Publication 4812 defines basic security controls, requirements and standards required of contractors (and contractor employees) when the contract is for services, contractors, and contractor employees who will either:

- Have access to, develop, operate, host, or maintain IRS SBU information or information systems for tax administration purposes (or provide related services) outside of IRS facilities or outside of the direct control of the Service, and/or
- Have access to, compile, process, or store IRS SBU information on their own information systems or that of a subcontractor or third-party Service Provider, or that use their own information systems (or that of others) and Electronic Information and Technology (as defined in FAR Part 2) to access, compile, process, or store IRS SBU information while working at an IRS owned or controlled facility.

SBU information includes all taxpayer returns and return information, as defined by Internal Revenue Code (IRC) Section 6103; all Personally Identifiable Information (PII), where there is information that can be associated to a specific individual; and other sensitive information to include, but not limited to Sensitive Law Enforcement Information, Employee Information, or other information protected by the Privacy Act, and organizationally sensitive information such as Information Technology (IT) system configurations, identification of vulnerabilities, etc.

Publication 4812 has been updated to include changes introduced by the NIST Special Publication (SP) 800-53 (Revision 4), Security and Privacy Controls for Federal Information Systems and Organizations.

Physical security controls have also been modified to clarify requirements at organizations housing IRS information.

Table of Contents

1 Background

The E-Government Act of 2002 (Public Law 107-347) Title III, Federal Information Security Management Act (FISMA) of 2002, as amended by Federal Information Security Modernization Act of 2014 (Public Law 113-283), requires each agency to provide security for "the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." FISMA requires federal agencies to develop and implement policies for information security oversight of contractors and other users with access to federal information and information systems.

To ensure FISMA compliance, the National Institute of Standards and Technology (NIST) identifies specific security controls/criteria in NIST Special Publication (SP) 800-53 (Revision 4), Security and Privacy Controls for Federal Information Systems and Organizations. NIST provides a series of recommended security controls to be employed by agencies and service providers to provide for the confidentiality, integrity, and availability of federal information and information systems and guidelines for effective security controls that support federal operations and assets.

Because of requirements distinct to IRS mission objectives, as well as specific laws or rulings, such as the Gramm-Leach Bliley (GLB) Act, the Federal Trade Commission (FTC) Financial Privacy Rule and Safeguards Rule, and the Sarbanes-Oxley Act, IRS contractors, their affiliates, subcontractors, and service providers are subject to additional requirements for protecting information and information systems, when appropriate or applicable.

2 Purpose

This publication defines basic security controls, requirements and standards that apply to contractors, contractor employees, and subcontractor employees supporting the primary contract, based on the security controls framework under NIST SP 800-53 (Revision 4), where those contractor employees have access to develop, operate, or maintain IRS information or information systems. While NIST SP 800-53 (Revision 4), is a general guide, the intent of Publication 4812 is to provide IRS security requirements in the IRS contracting environment.

This publication also describes the framework and general processes for conducting security assessments and responsibilities of the Government and the contractor in implementing security controls and safeguards to protect SBU information and information systems.

As described in NIST SP 800-53 (Revision 4), "The ultimate objective is to conduct the day-to-day operations of the organization and to accomplish the organization's stated missions and business functions with what Office of Management & Budget (OMB) Circular A-130 defines as *adequate security*, or security commensurate with risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information."

3 Scope

The requirements in this publication and the security controls contained hereinafter are based on NIST SP 800-53 (Revision 4).

3.1 IRS Security Controls Structure

NIST provides Federal agencies flexibility to apply the security concepts and principles in NIST SP 800-53 (Revision 4) within the context of and with due consideration to each agency's mission, business functions, and environments of operation.

As part of its information security program**,** IRS identifies security controls for the organization's information and information systems in the following two (2) key documents:

- Internal Revenue Manual (IRM) 10.8.1 – Information Technology (IT) Security, Policy and Guidance (The public document is redacted.), and
- Publication 4812 – Contractor Security Controls.

While IRM 10.8.1 and Publication 4812 are both based on NIST SP 800-53 (Revision 4), they apply to different operating environments – internal and external to the organization, respectively; and, as would be expected, vary greatly in the level of direct control the agency has over the host's or service provider's normal business operations.

3.1.1 IRM 10.8.1 Applicability

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. This manual also applies to individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, who have access to, and/or use or operate IRS information systems containing IRS information at facilities controlled by IRS. (Note: Beyond appropriate references to the manual, IRM 10.8.1 is outside of the scope of Publication 4812 and contractors who need to refer to that document for guidance may access it at http://www.irs.gov/irm/part10/irm_10-008-001.html.)

3.1.2 Publication 4812 Applicability

Publication 4812 is a layperson's guide of security controls specific to IRS, based on controls established in NIST SP 800-53 (Revision 4). Publication 4812 contains IRS-specific requirements that meet the standard for NIST SP 800-53 (Revision 4), and the security controls, requirements, and standards described herein are to be used in lieu of the common, at-large security control standards enumerated in NIST SP 800-53 (Revision 4). Contractors may, at their discretion, refer to NIST SP 800-53 (Revision 4), to gain a better understanding of the common standards, but shall coordinate with the Contracting Officer's Representative (COR) for their contract, or Pub4812@irs.gov, for clarification on Publication 4812 security controls/standards or guidance/requirements

specific to IRS. (Note: All NIST Special Publication (800 series) are available at the following web site: http://csrc.nist.gov/publications/PubsSPs.html.)

Publication 4812 defines basic security controls, requirements and standards required of contractors (and contractor employees) in which contractors and contractor employees (or subcontractors and subcontractor employees) will either:

- Have information systems for tax administration purposes (or provide related services) outside of IRS facilities or outside of the direct control of the Service, and/or
- Have access to, compile, process, or store IRS SBU information on their own information systems or that of a subcontractor or third-party Service Provider, or that use their own information systems (or that of others) and Electronic Information and Technology (as defined in FAR Part 2) to access, compile, process, or store IRS SBU information while working at an IRS owned or controlled facility.

Publication 4812 is typically incorporated into IRS contracts, agreements or orders (directly or through flow down provisions). IRS IT Security/FISMA Contract language is also included in any contracts or orders (directly or through flow down provisions) for IT acquisitions, which include IT hardware and/or software, telecommunications software or equipment, and maintenance/service (including consulting services) on any hardware and/or software products.

As used in this publication, the term “contract,” unless specified otherwise, includes (and the requirement or meaning of the text applies to) contracts, task/delivery/purchase orders, blanket purchase agreements, and interagency agreements in which IRS is the servicing agency and contractor services and resources, equipment and systems are being used to support the agreement. The publication may also be used and incorporated into interagency agreements in which IRS is the requesting agency and the servicing agency does not have a publication (or security controls consistent with NIST SP 800-53 (Revision 4)) in place comparable to Publication 4812.

As described in greater detail in subsequent sections, there are four (4) basic levels of security controls (from the first level requiring the least number of security controls and overall scrutiny, to the last level requiring the greatest number of security controls and overall scrutiny). One of which shall be assigned (or assignable) to all applicable service contracts, based on a number of risk-based factors (operators) that take into account and are responsive to individual users (e.g., individual, residential non-networked users) and business concerns of any size, with due deference to higher risk factors (operators) such as networked environments and software development. The specific security controls associated with each security control level can be found in Publication 4812, Section 8.4 and Publication 4812, Appendix C. The use of basic levels of security controls notwithstanding, IRS always reserves the right to add other security controls to any given contract to protect its assets–based on the work being performed, the environment in which the work is being performed, perceived risks

(threats and vulnerabilities), the suitability and effectiveness of existing controls, and other factors, as appropriate, and in the best interests of the Government.

Publication 4812 also describes the framework and general processes for conducting contractor security assessments to monitor compliance and assess the effectiveness of security controls applicable to any given contracting action subject to Publication 4812.

4 SBU Information

"SBU Information" as defined by OMB Circular No A-130 Revised, 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, 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.'

Access to SBU information shall be provided on a "need to know" basis. SBU information shall never be indiscriminately disseminated, and no person shall be given access to (or allowed to retain) more SBU information than is needed for performance of their duties, and for which that individual has been authorized to receive as a result of their having been successfully investigated and adjudicated, and trained to receive, and what is strictly necessary to accomplish the intended business purpose and mission.

SBU information shall only be released or accessible to those individuals who have been approved to receive such information (or in the case of information systems, approved for access) by IRS Personnel Security (PS), for interim or final staff-like access 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.

SBU shall be categorized in one (1) or more of the following groups:

- Returns and Return Information,
- Law Enforcement Sensitive (LES) Information,
- Employee Information,
- Personally Identifiable Information, and
- Other Protected Information.

4.1 Returns and Return Information

Returns and return information includes all information covered by § 6103 of the IRC, 26 U.S.C. § 6103. This includes tax returns and return information.

4.2 Law Enforcement Sensitive Information

This includes grand jury, informant, and undercover operations information and procedural guide.

4.3 Employee Information

All employee information covered by the Section 552a of Title 5, United States Code (USC) (5 U.S.C. 552A (g) (1). Examples include personnel, payroll, job applications, disciplinary actions, performance appraisals, drug tests, health exams, and evaluation data.

4.4 Personally Identifiable Information

The term “personally identifiable information” (PII) refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

OMB 07-16:
http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-16.pdf

PII includes the uniquely identifiable personal information of taxpayers, employees, contractors, applicants, and visitors to the IRS. Examples of PII include, but are not limited to:

- Name,
- Home address,
- Social Security number,
- Date and place of birth,
- Mother’s maiden name,
- 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.

PII includes any information related to an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information, to distinguish or trace an individual's identity as shown above. This is discussed in the Incident Handling section 18.4, IR-4 Incident Handling of this document.

4.5 Other Protected Information

Other protected information includes any knowledge or facts received by or created by IRS in support of IRS work. This includes all information covered by the Trade Secrets Act, the Procurement Integrity Act, and similar statutes. Examples include, but are not limited to:

- Records about individuals requiring protection under the Privacy Act,
- Information that is not releasable under the Freedom of Information Act,
- Proprietary data,
- 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,
- Information related to the design and development of application source code,
- For contracting organizations providing IT support to the IRS, this includes specific IT configurations, where the information system security configurations could identify the state of security of that information system; Internet Protocol (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,
- Security information containing details of serious weaknesses and vulnerabilities associated with specific information systems and/or facilities, and
- Any information, which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

5 Information and Information Systems

Information requires protection whether or not it resides on an information system.

Per OMB Circular A-130 (Section 6, Paragraph j), the definition of Information is as follows:

The term "information" 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.

Information System, as defined by OMB Circular A-130, means “a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.”

In all instances, security controls apply to both information and information systems.

6 Disclosure of Information

Disclosure of returns and return information is generally prohibited unless authorized by statute. The IRC makes the confidential relationship between the taxpayer and the IRS quite clear, and stresses the importance of this relationship by making it a crime to violate this confidence. Designed to protect the privacy of taxpayers, IRC Section 26 U.S.C. § 7213 prescribes criminal penalties for contractors and their contractor employees who make unauthorized disclosures of returns and return information and Privacy Act protected information. (Note: IRC Section 26 U.S.C. § 7213 criminal

penalties do not apply to PII information unless it falls under the banner of tax information.) The sanctions of the IRC are designed to protect the privacy of taxpayers.

Additionally, IRC Section 26 U.S.C. § 7213A makes the unauthorized inspection of returns and return information a misdemeanor punishable by fines, imprisonment, or both. And finally, IRC Section 26 U.S.C. § 7431 allows for civil damages for unauthorized inspection or disclosure of returns and return information, and upon conviction, the notification to the taxpayer that an unauthorized inspection or disclosure has occurred. IRC Section 26 U.S.C. § 6103 (n) gives the contractor the authority to disclose returns and return information to its employees whose duties or responsibilities require the returns and return information for a purpose described in paragraph (a) of the section. Prior to releasing any returns and return information to a subcontractor, the contractor must have written authorization from the IRS.

Contractors shall have adequate programs in place to protect the information received from unauthorized use, access, and disclosure. The contractor's programs for protecting information received must include documenting notification to employees and subcontractors (at any tier), who will have access to SBU information, the importance of protecting SBU information in general, and returns and return information, and information protected by the Privacy Act in particular. The documented notification must also include the disclosure restrictions that apply and the criminal or civil sanctions, penalties or punishments that may be imposed for unauthorized disclosure or inspection. Disclosure practices and the safeguards used to protect the confidentiality of information entrusted to the Government (and, as provided under the IRC and the Privacy Act) are subject to continual assessment and oversight to ensure their adequacy and efficacy.

7 Roles and Responsibilities

The following sections define roles and responsibilities in the contractor assessment process.

7.1 Government

7.1.1 Contracting Officer (CO)

- Enforces the government's rights and remedies for all contractual matters.
- Ensures compliance with the terms and conditions of the contract.
- Ensures appropriate security-related clauses and language are included in applicable contracts.
- Ensures the contractor affords the Government access to the contractor's facilities, installations, operations, documentation, records, IT systems, and databases to carry out a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of Government data. The Government shall perform inspections and tests in a manner that shall not unduly delay the work.
- Employs all rights and remedies available to the Government to ensure contractors take action to correct or mitigate identified security vulnerabilities.

- Modify contract, when risk level requires modification, based upon Cybersecurity recommendation.

7.1.2 Contracting Officer's Representative (COR)

- Reviews the information provided in the State of Security Package for accuracy.
- Facilitates contractor security reviews and serves as the liaison between the Contractor Security Assessments (CSA) team and the contractor when scheduling contractor security assessments and by being the primary IRS focal point for the contractor.
- Escalates key information to the Contracting Officer related to contractor risk.
- Provides quarterly status of the Plan of Action and Milestone (POA&M) to Cybersecurity.
- Furnishes the Security Assessment Report (SAR) and related information to the contractor.
- Identifies to the contractor, the names of specialized IT Security Roles and the associated number of required hours for specialized Security Training.
- Provides a copy of the Privacy and Civil Liberties Impact Assessment (PCLIA) to the contractor and identifies any specific requirements required by the contractor, when a PCLIA is required.

7.1.3 Information Technology and Contractor Security Assessments (CSA)

- Establishes the schedule for Contractor Security Assessments in coordination with COs, CORs and targeted contractors.
- Conducts Contractor Site Assessments (and virtual site assessments, when appropriate) for the current FISMA year cycle (July 1st to June 30th).
- Coordinates with the COR to identify contractor security review timeframes to conduct assessments.
- Maintains and updates, as appropriate, Publication 4812 and related materials (e.g., Contractor Statements of Security Assurance (CSSA), State of Security (SoS) Package content and format, and guidelines for examining such materials), and coordinates changes or updates with Procurement and other organizational components and stakeholders.
- Acts as a resource for CORs/ Business Operating Division (BODs) in developing POA&Ms and assessing compliance, and reconciliation or mitigation efforts.
- Acts as a point of contact for technical issues for BODs and Procurement Officials (and directly or indirectly for contractors). IT/CSA can be contacted at Pub4812@irs.gov.
- Furnishes SARs and appropriate briefings to contractors who are the subject of Contractor Security Assessments, and to BODs, COs, and CORs.
- Alerts Situation Awareness Management Center (SAMC) of any incidents, risks, or vulnerabilities discovered in the course of conducting a Contractor Security Assessment that represents immediate, actionable threat intelligence, or presents an unusually urgent demand for attention, correction, or remediation. Similarly, alerts Disclosure, Facilities Management and Security Services (FMSS), Procurement, PGLD, or others, as appropriate, of issues of a pressing

nature revealed in the course of conducting a Contractor Security Assessment that falls within each component's areas of responsibility.

7.1.4 Privacy, Governmental Liaison and Disclosure (PGLD)

- Preserves and enhances public confidence by advocating for the protection and proper use of identity information.
- Promotes the privacy and protection of personally identifiable information in the trust of the IRS by integrating privacy protections in technology solutions and business practices.

7.1.5 Agency Wide Shared Services and Facilities Management and Security Services (AWSS/FMSS)

- Ensures readiness and preparedness activities enhancing IRS's ability to continue ongoing services to taxpayers.
- Trains and supports IRS employees and contractors to adequately protect locations and sensitive information where IRS work is performed (FMSS Physical Security).
- Prepares and disseminates SAMC Incident Reports accordingly.
- Collaborates with CSA to conduct physical security portion of the Contractor Security Assessment.

7.1.5.1 Contractor Security Management (CSM)

- Initiates and monitors investigative processing for all contractors for IRS contracts.
- Ensures Security Awareness Training (SAT) is provided to contractors annually, and tracked.
- Ensures Specialized Information Technology Security (SITS) training is tracked.
- Reports the number of contractors that complete the mandatory SAT and SITStraining to IT Cybersecurity.

7.1.6 Personnel Security (PS)

- Receives and processes all investigative processing requests from CSM.
- Notifies the appropriate IRS stakeholders of any changes to access status.
- Intakes and assesses Position Designation Surveys from contractors (directly or through the COR), and uses the Office of Personnel Management Position Tool to assign the position risk designation (or make adjustments/updates, as needed) prior to granting contractor personnel interim or staff-like access to IRS information or information systems.

7.1.7 Project Manager/Task Manager

- Performs Privacy Threshold Analysis by filling out the PCLIA Qualifying Questionnaire and emailing the completed form to *** Privacy**
- Forwards the PCLIA form to the COR, if Privacy determines a PCLIA is required
- Reviews findings and collaborates with the contractor to develop a Plan of Action and Milestone (POA&M) to correct or remediate identified risks.

- Coordinates with the contractor to update POA&M and provide updates to COR quarterly.

7.2 Contractor

In order to ensure IRS information and information systems are protected at all times, it is the responsibility of IRS contractors to develop and implement effective controls and methodologies in their business processes, physical environments, and human capital or personnel practices that meet or otherwise adhere to the security controls, requirements and objectives described in this publication, and their respective contracts. As part of the award process, the contractor is required to include an assigned 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 of contact 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.

Whenever PII is being collected by a contractor, the contractor is responsible for protecting this information as identified in the IRS Privacy and Civil Liberties Impact Assessment (PCLIA).

7.2.1 Contractor Security Representative (CSR)

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

Significant responsibilities shall include but may not be limited to contractor employees who have access to either contractor-managed facilities or contractor managed systems/IT assets used to handle, process or store IRS SBU information, regardless of location or facility, to include contractors who need such access including the use of other IT resources, at contractor managed facilities.

The CSR is responsible for ensuring the following responsibilities are addressed through the life cycle of the contract. Specific roles and responsibilities shall include:

- Complete and submit the State of Security (SOS) package
- At least quarterly, provide updates to the CO/COR on all identified findings using POA&Ms
- Report all incidents to the IRS, as required under Incident Reporting section of this document.
- Ensure all employees undergo the necessary security screening process and receive interim or final staff-like access approval prior to beginning work under the awarded contract or order. Ensure all employees take required IRS training annually related to the protection of information.

- Complete the PCLIA, if provided by the COR.

7.2.2 Contractor Employees

- Ensure all training is completed annually as required by contractor management.
- Ensure all security policies and procedures are followed during routine work.
- Ensure the safeguarding of all information provided to the contractor as part of the IRS contract.

7.3 Contractor Program Requirements

The contractor must develop a comprehensive security program that addressees all aspects of IT security.

7.3.1 Contractor Security Policies and Procedures

Contractors are responsible for developing processes and putting in place procedures to implement security controls and requirements in this publication and the contract.

As described in NIST SP 800-53 (Revision 4) the first security control in each family is also known as the "*dash one (1)"* control (e.g., AC-1, CP-1, SI-1, etc.). It generates the requirement for policy and procedures that are needed for the effective implementation of the other security controls and control enhancements in the family.

A contractor who is subject to the security controls under Publication 4812 does not necessarily have to develop a plan specific to each family if and when those policies and procedures are already established in some existing formal or institutional document that the contractor can readily identify (to the satisfaction of IRS), and the plan contains policies and procedures that address the material elements or requirements for that particular dash one (1) control and security control family. For example, if the PS-1–Personnel Security Policy and Procedures requirements for a formal documented personnel security policy (and procedures to implement those polices and associated personnel security controls) are already contained in the contractor's existing Human Resources policies, the contractor would not have to recreate this documentation so long as the IRS determines (or is in a position to determine) these existing products or records fulfill the key, germane aspects and requirements for that particular dash one (1) control, as specified in Publication 4812.

Only when the contractor does not have standing policies and procedures that adequately and fully address each respective security control family dash one (1) requirement (or the existing policies and procedures are inadequate and need to be supplemented), does the contractor need to develop specific policies and procedures to address that particular control family.

7.3.2 Contractor Investigative Requirements

All contractors, subcontractors, experts, consultants, and paid/unpaid interns, like Federal employees, are subject to a security screening to determine their suitability and fitness for Department of the Treasury or IRS work, and the security screening must be favorably adjudicated. The level to which such contractor personnel and others are screened or investigated shall be comparable to that required for Federal employees

who occupy the same positions and who have the same position sensitivity designation. Security screening is required regardless of the location of the work. This includes contractor or subcontractor employees who use technology for remote access to information technology systems as well as those who have direct physical access to any IRS documents or data outside of any IRS facility.

Contractors shall ensure all contractor and subcontractor employees performing or proposed to perform under the contract are identified to the IRS at time of award (or assignment) in order to initiate appropriate security screening.

Contractors shall ensure that any personnel that are not favorably adjudicated or otherwise pose a security risk are immediately removed from performance under contracts with the IRS, and suitable replacement personnel agreeable to the IRS are provided.

7.3.3 Contractor Training

Ensure all contractor employees who require staff-like access to IRS information or information systems, where these are located at contractor managed facilities using contractor managed assets; regardless of their physical location complete the required Security Awareness Training. Contractor activities that require IRS security awareness training include but are not limited to:

- Manage, program or maintain IRS information in a development, test or production environment.
- Manage or operate an information system or IT asset for tax administration purposes.
- Conduct testing or development of information or information systems for tax administration purposes.
- Provide information system administrative support.

Maintain and furnish, as requested, records of initial and annual training and certifications. Establish additional internal training, as needed (or as required under the terms of the contract), for personnel in the organization who require access to IRS information or information systems to perform under the contract.

Please reference Section 12.2 AT-2 Security Awareness Training, for time requirements to complete training.

7.3.4 Contractor Information Protection

Ensure all SBU information is protected at rest, in transit, and in exchanges (i.e., internal and external communications). Limit access to SBU information to authorized personnel (those favorably adjudicated and trained) with a need to know, and ensure internal and external exchanges are conducted only through secure or encrypted channels. The contractor shall employ encryption concepts and approved standards to ensure the confidentiality, integrity, and availability of the SBU information, consistent

with the security controls under Publication 4812 and any security requirements specified elsewhere in the contract.

7.3.5 Rules of Behavior

Contractors shall develop and distribute a set of internal rules of behavior with regard to access to and use of Government information and information systems. Rules of Behavior, which are required in OMB Circular A-130, Appendix III, and is a security control contained in NIST SP 800-53 (Revision 4), shall clearly delineate responsibilities and expected behavior of all individuals with access to information systems and/or Government information and/or IRS SBU information. The rules shall state the consequences of inconsistent behavior or noncompliance, and be made available to every user prior to receiving authorization for access to the system and/or IRS SBU information. It is required that the rules contain a signature page for each user to acknowledge receipt, indicating that they have read, understand, and agree to abide by the rules of behavior. Electronic signatures are acceptable for use in acknowledging the rules of behavior. Contractors must maintain (and furnish, as requested) records of signed acknowledgements on the rules of behavior, Non-Disclosure Agreements, and completion of all required security awareness training.

8 Contractor Security Assessments (CSA)

8.1 Overview

Security controls are the management, operational, and technical safeguards or countermeasures employed to protect the confidentiality, integrity and availability of an organization's information and information systems.

Contractor Security Assessments are on-site evaluations performed by the IRS to assess and validate the effectiveness of security controls established to protect IRS information and information systems. Security control effectiveness addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to protecting information and individual privacy, or meeting the security requirements for the information system in its operational environment. These assessments help to determine if and when additional controls or protections are necessary to protect returns and return information or personal privacy, or other SBU information, and organizational assets and operations.

All contracts subject to this publication are subject to an on-site Contractor Security Assessment each annual review cycle (i.e., the 12 month period beginning July 1st of each year, coinciding with the beginning of the FISMA calendar year).

Contractor Security Assessments are conducted by IRS and cannot be a self-assessment performed by the contractor. Contractor Statements of Security Assurance (CSSA) that are completed by contractors, as described herein after provide the means for the contractor to make a preliminary assertion to the IRS as to its perceived level of conformity to security requirements. Such assessments/assertions can provide contractors further insight into their own operating environments, and serve as one (1)

of the tools used to determine if and when a Contractor Security Assessment will be performed by the IRS on any given contract, in any given annual assessment cycle.

8.2 Types of Assessments

As a general rule, the current contract conditions and stage of the acquisition lifecycle will dictate the type of Contractor Security Assessment the IRS will conduct. Qualifying events or conditions that may prompt or necessitate the IRS perform a security assessment include:

- Pre-Award Assessments: Pending the award of a contract, the IRS may require that the apparently successful offeror provide verification (or be subject to verification by IRS) that security controls are in place, as built into the solicitation. With due consideration to the scope of the contract, and the urgency and immediacy of need for access to (and release of) SBU information and/or information systems, and other factors, as a general rule, IRS will not conduct pre-award assessments, but reserves that option.
- Immediate (Probationary) Post–Award Assessments: This type of assessment may be conducted within the first 30–90 days of award, and may be performed in lieu of a pre-award assessment when award is imminent and the need to make the contract award is urgent and compelling, but conducting a pre-award assessment is not viable. In such cases, the IRS would have determined that the award may proceed, and that IRS approved interim access to information or information systems is allowable, but that an assessment is necessary as soon as possible after award.
- Periodic Post–Award Assessments: Based upon the type of work being performed and the volume of SBU being processed, the IRS may schedule an assessment, at least annually, to ensure security controls are in place, and operating as intended.
- End of Contract Assessments: At contract expiration or termination, the IRS may elect to conduct a security assessment to ensure that all IT resources and SBU data have been adequately inventoried and returned or disposed of in accordance with the contract.

8.3 Notice of Assessments

For each contract the IRS selects for assessment in any given annual assessment cycle, the IRS will advise the contractor of the Service's intent to conduct an on-site Contractor Security Assessment. As a general rule, approximately one (1) month prior to the projected timeframe or proposed date of the assessment, the IRS will coordinate a mutually agreed upon assessment date to visit the contractor's facility or work site. This advance notice is as much a courtesy as it is recognition of the planning and preparations required by both the IRS and the contractor. It does not however preclude the IRS from conducting unannounced assessments or reviews on short notice (in a manner not to unduly delay the work).

Typically, on–site Contractor Security Assessments are one (1) to three (3) days in duration, whereas virtual assessments (by telephone or other telecommunication channel) for applicable contracting actions usually will not exceed one (1) day.

The notice of a pending assessment (i.e., letter of intent) will also include a data call for supporting documentation evidencing the security controls in place and in use. (Note: The letter will specify what, if any, documentation should be furnished prior to the site visit.)

8.4 Security Control Levels

Contractor sites and work environments using IT assets to access, process, manage, or store SBU information under contracts to IRS will likely vary in size, number of users and complexity. For this reason, the IRS has established minimum and advanced sets of security controls that are selected, depending upon the complexity of the contract, cost, and other factors. As described in more detail in the following subparts, four (4) control sets are categorized (within the assigned moderate impact designation) as follows:

- Core Security Controls (C),
- Core (C) + > Simplified Acquisition Threshold (SAT),
- Core (C) + Networked Information Technology Infrastructure (NET), and
- Core (C) + Software Application Development or Maintenance (SOFT).

High Water Mark: Publication 4812 uses what is in effect, a “high water mark” concept in which operators or conditions surrounding the complexities of the work activity and the IT environment in which performance occurs have a higher precedence over lower, less complex operators of dollar value and duration of the contract. As such, more (and more complex) security controls are contained in the higher security control levels (in descending order— CSOFT, CNET, and CSAT), all of which build on and include the lower, preceding security control level (and its set of controls) starting with the basic security control level C (Core), which applies to all contracting actions for services that are subject to Publication 4812, as described in Section 3.

Operators: The pre-defined conditions or operators for determining and applying security control levels/security controls are as follows (in descending order of precedence and logical progression):

- Development Activity (highest operator): Contracts that involve software or application development, design, maintenance, or related support services,
- IT System Environment: A contractor that operates in and/or houses IRS information on a contractor network environment infrastructure (in short, an interconnected group of computer systems linked by the various parts of a telecommunications architecture) *versus* a contractor that operates in a standalone mode (and houses IRS information), on a non-networked computer,

- Dollar Value: Dollar value of the contract (inclusive of the value of all options) with the Simplified Acquisition Threshold (SAT) being a breakpoint (with higher level controls applied to actions valued above the SAT), and
- Duration (lowest operator): Duration of the contract (inclusive of the periods of performance of all options) with one (1) year being a break point (with higher level/additional controls applied to actions that are of duration of more than one (1) year, inclusive of any and all options).

Under this order of precedence (or predominance), when two (2) or more operators (for example, IT system environment and dollar value) are present, the operator with higher precedence is employed, and takes priority over (and incorporates) the operator(s) requiring a lesser degree of scrutiny. In the example, dollar value is of lesser precedence and subordinate/secondary to IT system environment. As such, a greater amount of scrutiny is required, and the higher level security controls applicable to an IT system environment are used.

Security Control Levels: Publication 4812 employs the following four (4) security levels (within the assigned impact designation applicable contracting actions; which are moderate, by default):

1. **C**ore (C) Security Controls
   (Abbreviated "**C**")

   All contracting actions for services that involve contractor access to SBU information and/or information systems must include the core security controls.

   Core (**C**) security controls typically apply to:

   - Contracts to an individual (e.g., expert witness, appraiser),
   - Contracts of 1 year or less duration, inclusive of all options, or
   - Contracts valued at or less than the SAT, inclusive of all options (or for Indefinite Delivery contracts and BPAs that allow for placing orders, the estimate value of the order, inclusive of all options).

   Examples of contracts in this category include experts in a subject area such as valuations, property assessments, or legal services.

   The need for higher level security controls is determined when other (higher order/precedence) operators, or conditions and factors exist.

2. **C**ore (C) plus value greater than **S**implified **A**cquisition **T**hreshold (SAT)
   (Abbreviated "**CSAT**")

   CSAT security controls typically apply to:

Contracting actions for services that involve contractor access to SBU information and/or information systems, by any contractor (individual or business concern), that are valued above the SAT, inclusive of all options, irrespective of the duration of the contract. Such contracts will include and be subject to both the core security controls, and CSAT security controls.

Examples of this type of environment could include research teams working primarily independently but sharing SBU data. Another example would include a stand-alone device used by more than one (1) user through a time-sharing arrangement. In some cases, research teams shall store mission source data and project deliverables on a stand-alone platform. Project members would then access the central store to extract project documents or data sets for analysis.

The need for higher level security controls is determined when other (higher precedence) operators, or conditions and factors exist.

3. **C**ore (C) plus **Net**worked Information Technology Infrastructure (NET) (Abbreviated "**CNET**")

   Contracting actions for services that involve contractor access to SBU information and/or information systems, by any contractor (individual or business concern) that has a networked IT infrastructure (in short, an interconnected group of computer systems linked by the various parts of a telecommunications architecture). Contracting actions that utilize a networked IT infrastructure, regardless of dollar value, and irrespective of the duration of the contract, must include the core security controls, and CNET security controls.

   Examples of a networked infrastructure include:

   - IRS information is maintained on a file or shared area, where access controls are used to manage access to the file or shared area.
   - IRS information is maintained on a file that is shared among multiple employees who all have authority and need to know to access and maintain the information.

   The need for higher level security controls is determined when other (higher precedence) operators, or conditions and factors exist.

4. **C**ore (C) plus **Soft**ware Application Development/Maintenance (SOFT) (Abbreviated "**CSOFT**")

   Contracting actions for services that involve contractor access to SBU information and/or information systems, by any contractor (individual or business concern) that entails software application development, maintenance, or related support service, regardless of dollar value, and irrespective of the duration of the contract, must include the core security controls, and CSOFT security controls.

An example of this type of contract or environment includes contractor sites, where multiple employees have access to IRS SBU information and/or IT assets and where this information is being accessed on information systems in a networked environment. In addition, the contractor is providing support to develop software, perform testing, and perform information system maintenance or other related support service.

Appendix C of this volume provides specific detail on the controls contained in each of these levels.

8.5 Scope of Assessments

Contractor Security Assessments typically concentrate on the following key areas:

- Information or information systems,
- Physical environment in which the information system or information is handled or processed, and
- Personnel who have access to or are responsible for handling or processing the information system or information.

A Security Assessment Plan will typically accompany the letter of intent. The plan will include greater specificity on the types of assessments that will be employed, and the areas or activities the CSA team intends to assess as part of its assessment, such as:

- Evaluation of all applicable Publication 4812 security controls.
- Verification of all personnel security background investigations for all contractor employees working on the IRS contract, including subcontractor employees, and IT support personnel (at any tier) that have access to SBU information or information systems.
- Validation of IT security configurations including workstations, servers, routers, and switches.
- Verification of employee's completion of IRS mandated Security Awareness Training, which is based on completion of various Information Protection briefings (on an annual basis) on information system security, disclosure, privacy, physical security, and/or unauthorized access (UNAX) – 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.
- Performance of vulnerability scans, as necessary, for public facing web servers.
- Preliminary identification of any weaknesses, threats or vulnerabilities, with more details to be provided in a Security Assessment Report (SAR) at a later date.

8.5.1 Collaboration on Contractor Security Assessments

8.5.1.1 Before the Assessment

Contractors shall coordinate with the IRS on all aspects of preparation of the assessment to include, but not limited to, agreement on time(s) and place(s) of assessment, and timely submission of any pre-site visit materials, as requested, and

making ready for inspection, all other policies, documentation, and records that shall be needed at the time or during the assessment.

8.5.1.2 At the Time of, or During the Assessment

The contractor shall make its facilities, installations, operations, documentation, records, databases, and personnel available to the IRS to carry out a program of inspection (in a manner not to unduly delay the work) to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of Government data.

Access to contractor facilities and IRS information or information systems by IRS inspectors/assessors (e.g., CORs and CSA Team) shall be permitted, in accordance with the terms of the contract, subject to confirmation of identity, which shall be based on each person presenting an active (unexpired), Government issued Personal Identity Verification card. PII such as a Social Security Number or Date of Birth shall not be needed for or requested of Government personnel conducting an inspection/assessment. A contractor facility that maintains classified information and is subject to the National Industrial Security Program, and that has additional Government mandated protocols for access must identify those requirements in writing to the IRS, for its consideration, not less than 10 days before the scheduled inspection/assessment. Denial of access to the Government to conduct its inspections may violate the terms of the contract and constitute a breach of contract.

8.5.1.3 After the Assessment

Within 45 days of the completion of the Contractor Security Assessment, the assessor, the CSA Team, shall furnish the CO/COR a final copy by recommendation of its information system and program of security in the form of a SAR. The CO/COR shall furnish copies of the SAR to the contractor.

The SAR contains:

- Results of the security assessment. This typically includes:
  - Findings of *met* or *not met* (with respect to meeting or not meeting individual security controls standards/requirements).
  - Identification of the parts of the security control that did not produce a satisfactory result or that may have the potential to compromise IRS information or the contractor's information system.
  - A critique on the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
  - An assessment on the organization's overall effectiveness in providing adequate security.
- Recommendations for correcting deficiencies in the security controls and reducing or eliminating identified vulnerabilities.

The SAR is a key element used in developing a POA&M. The POA&M is a management process and tool developed by the Government and the contractor (which may be based, in part, on the contractor's internal corrective action plan) that outlines

weaknesses or deficiencies identified in the Contractor Security Assessment and noted in the SAR, and delineates the tasks necessary to correct, remediate, or mitigate less than satisfactory findings in the SAR.

The contractor shall collaborate with the IRS in developing the POA&M, prioritizing the identified weaknesses/deficiencies for corrective actions, and identifying the actions to be taken within an agreed upon, realistic schedule (within the period of performance or life of the contract) to correct or effect desired changes in any weaknesses or deficiencies identified in the SAR and/or POA&M. The contractor shall track and furnish IRS status or progress reports, as directed.

8.5.2 Continuous Monitoring of Security Controls

Contractors must maintain ongoing awareness of their information system and related security control processes to ensure compliance with security controls and adequate security of information, and to support organizational risk management decisions. Continuous monitoring of organizations and information systems to determine the ongoing effectiveness of deployed security controls, changes in information systems and environments of operation, and compliance with legislation, directives, policies, and standards.

8.5.3 State of Security Package

For all contracts subject to this publication (see section/paragraph 3.1.2 above) that are 12 months or more in duration (inclusive of the base period and/or any exercised option periods), the contractor will advise the COR of the availability of the SoS and provide access for the COR's review
The SoS Package shall be furnished to the COR (or the CO if no COR is appointed) no later than 60 calendar days after the effective date of the contract in the base period (typically, the award date, unless specified otherwise), and on or before the annual anniversary of the effective date of the contract in each exercised option period. Note: If the base period is less than 60 calendar days in duration, the initial submission is still due within 60 days of the effective date of the contract (although it technically falls in the first option period), and the next submission is still due on or before the annual anniversary of the effective date of the contract (although it too technically falls in the first option period).

The SoS Package is comprised of the following components:

- Form 14419B State of Security (SoS) Questionnaire,
- Form 14419 Contractor Statements of Security Assurance (CSSA),
- Form 14419A Contractor Statements of Physical Security Assurance (CSPSA) and,
- System Security Plan (SSP).

Any questions regarding the SoS Package can be sent to Pub4812@irs.gov. The SoS Package can be found at http://www.irs.gov/uac/Publication-4812-Contractor-Security-Controls.

8.5.3.1 SoS Security Questionnaire (Form 14419B)

- Administrative Information Cover: Includes information such as date completed, contractor name, location of facilities handling IRS SBU information or information systems, place of facility if different from location of facility, points of contact (e.g., Contractor Security Representative, Project Manager, System Administrator) and their telephone numbers and email addresses, contract/order number, period(s) of performance, dollar value (by period(s) of performance) and business size.
- Security Environment Indicators: Series of closed ended questions designed to give the IRS a general picture of the work environment.
- Subcontractor Information: Identification of subcontractors who shall (a) have access to, or develop, operate, or maintain IRS SBU information or information systems outside of IRS controlled facilities or the direct control of the service, and/or (b) have access to, compile, or store IRS SBU information on the prime contractor's information systems, their own information systems, or that of a third-party Service Provider.
- Service Providers: Identification of any personnel used to provide IT services, or other services, such as network installation, network management, etc.
- IT Environment: A series of closed ended questions that provide security configuration results for IT resources, including workstations, servers, routers, switches, etc.

8.5.3.2 Contractor Statements of Security Assurance (IRS Form 14419)

The IRS shall employ CSSAs as part of an integrated security management approach to proactively mitigate security risks. The IRS shall use a staged report card or traffic light information system in its assessment of contractor reporting to augment compliance assessments (i.e., Contractor Security Assessments).

CSSAs are not required for contracts subject to Publication 4812 that are less than 180 days in duration. CSSAs are required for all contracts subject to Publication 4812 that are between 180 days and 12 months in duration and in which there are no options to extend the term of the contract. Contractors in this group are required to submit a CSSA to the COR during the period of performance according to the following schedule:

- For contracting actions with a start date on or after July 1st, not later than December 31st of that same year, or 180 days after the award date; whichever date is later;
- For contracting actions with a start date after January 2nd, not later than June 30th of that same year, or 180 days after the award date, whichever date is later.

The CSSA, available at the following site http://www.irs.gov/uac/Publication-4812-Contractor-Security-Controls, is in the format of an electronic questionnaire that includes a dropdown menu that allows the user to select the version of the CSSA associated with the security control level applicable to the immediate contract. This meets the annual submission requirements.

8.5.3.3 Contractor Statements of Physical Security Assurance (CPSA- IRS Form 14419-A)

The CSPSA is the IRS security management approach to the Physical Security in proactively mitigating security risks. The CSPSA is a companion form to the CSSA (see paragraph 8.2.10.2) and is also required as part of the SoS Package.

The CSPSA, available at the following site http://www.irs.gov/uac/Publication-4812-Contractor-Security-Controls, is in the format of an electronic questionnaire that includes a dropdown menu that allows the user to select the version of the CSPSA associated with the security control level applicable to the immediate contract.

8.5.3.4 System Security Plan (SSP)

Security Control PL-2 describes the contents of the System Security Plan and furnishes additional guidance.

9 Security Categorization

The Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, establishes security categories for both information and information systems. The information system impact level is derived from the security category in accordance with FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. FIPS 200 and NIST SP 800-53 (Revision 4), in combination, help ensure that appropriate security requirements and security controls are applied to all federal information and information systems.

As required by FIPS 200, organizations use the security categorization results to designate information systems as low-impact, moderate-impact, or high-impact systems.

The IRS has determined the security impact for all contracting actions subject to Publication 4812 is moderate-impact, unless:

- The information system in the contract to which the contractor has staff-like access is one (1) of the limited number of systems on the IRS FISMA Inventory (i.e., it is specifically identified as such, and/or it is a major application or general support system, as defined by OMB Circular A-130, Appendix III). In this case, Publication 4812 would be replaced with the more stringent standards for a high impact system, and other requirements as may be specified by IRS.
- A different impact level is specified in the contract (at time of award, or by modification).

The security impact level can only be lowered if and when IT Cybersecurity determines, in writing, all three (3) of the security objectives (confidentiality, integrity, and availability) are low. The security impact level shall only be raised if and when IT Cybersecurity determines, in writing, any one (1) of the three security objectives is high.

In the event the impact level is to be lowered or raised from moderate impact for any contract that is subject to Publication 4812, the change shall be reflected in the contract at time of award or by modification of the contract. At such time, security control requirements appropriate to the new impact level shall be provided to the contractor (e.g., guidance on any security controls or control enhancements from the default standard (moderate-impact) that do not apply (or are lessened), if and when the impact level is being lowered to low-impact; or additional controls or control enhancements above the default standard (moderate-impact) that would apply, if and when the impact level is being raised to high-impact.)

10 Security Control Organization and Structure

This document provides required controls for protecting SBU information, developed from the NIST guidance. The security controls in this document are organized into families as described in NIST SP 800-53 (Revision 4). Each security control family contains security controls related to the functionality of the family. A two-character identifier is assigned to uniquely identify each security control family.

The following table summarizes the control families, and associated identifiers for developing security controls used in this publication.

Table 1: NIST Families of Security Controls

IDENTIFIER	FAMILY
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity

IDENTIFIER	FAMILY
AR, DM, SE	Privacy

Of the eighteen security control families in NIST SP 800-53 (Revision 4), seventeen families are described in the security control catalog in Appendix F of the NIST publication, and are closely aligned with the seventeen minimum security requirements for federal information and information systems in FIPS 200. One additional family, (Program Management [PM] family), in Appendix G of NIST SP 800-53 (Revision 4), provides controls for information security programs. This family, while not referenced in FIPS 200, provides security controls at the organizational level rather than the information system level. The PM controls address the strategic level implementation of an overall security program. Contractors subject to Publication 4812 are not responsible for the implementation of IRS strategic security program management.

There are a number of controls that have either been withdrawn or are not selected. As a result, these controls are not described in this document. The following table lists these withdrawn or not selected controls.

Table 2: Withdrawn or Not Selected Security Controls or High Impact Security Controls

AC-9	CA-4	PE-20	SA-15	SC-14	SC-36	AR-8
AC-10	CA-8	PL-3	SA-16	SC-16	SC-37	
AC-13	CP-5	PL-5	SA-17	SC-24	SC-38	
AC-15	CP-11	PL-6	SA-18	SC-25	SC-40	
AC-16	CP-12	PL-7	SA-19	SC-26	SC-41	
AC-23	CP-13	PL-9	SA-20	SC-27	SC-42	
AC-24	IA-9	RA-4	SA-21	SC-14	SC-43	
AC-25	IA-10	RA-6	SA-22	SC-29	SC-44	
AT-5	IA-11	SA-6	SC-3	SC-30	SI-6	
AU-10	IR-9	SA-7	SA-15	SC-31	SI-9	
AU-13	IR-10	PE-20	SA-16	SC-32	SI-13	
AU-14	MP-8	SA-12	SC-6	SC-33	SI-14	
AU-15	PE-18	SA-13	SC-9	SC-34	SI-15	
AU-16	PE-19	SA-14	SC-11	SC-35	SI-17	

11 Access Control and Approving Authorization for IT Assets (AC)

Access controls provide security controls required to restrict access to information and to information systems. Information shall be restricted to those contractors who have a valid background investigation with interim or final approval and a need to know.

11.1 AC-1 Access Control Policy and Procedures

For all contractors who have IT assets (i.e., information system or server) the contractor shall develop access control policies and procedures. The contractor shall develop, document, disseminate, and review/update policies and procedures annually or if there

is a significant change to ensure adequate access controls are developed and implemented.

11.2 AC-2 Account Management

Any time there is more than one (1) contractor using an IT asset, such as a server, network, or information system, the contractor shall assign an account manager for the IT asset and configure the asset so that there is one (1) unique account created and used for each employee who shall perform IRS work on that asset.

There shall be a procedure that briefly describes how these accounts shall be established, reviewed at least annually (semi-annually for privileged accounts), modified, or deleted, as necessary. At a minimum, the contractor shall identify all personnel authorized to access the IT asset, including information system support personnel.

The contractor shall notify account managers:

- When accounts are no longer required;
- When users are terminated or transferred; and
- When individual information system usage or need-to-know changes

Control Enhancements:

- The contractor shall employ automated mechanisms to support the management of IT asset accounts.
- The information system shall automatically remove/terminate temporary and emergency accounts after two (2) business days.
- The information system shall automatically disable inactive user accounts after 120 days of inactivity.
- The information system shall automatically disable administrator accounts after 60 days of inactivity.

The information system shall automatically audit account creation, modification, enabling, disabling, and removal termination actions and notifies, as required, appropriate individuals.

11.3 AC-3 Access Enforcement

The contractor shall develop a process that demonstrates how contract employees are approved for access, prior to being authorized access to IT assets used for IRS work.

Note: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by the contractor to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in an information system.

11.4 AC-4 Information Flow Enforcement

The contractor shall regulate where information is allowed to travel within an information system and between interconnected information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information.

11.5 AC-5 Separation of Duties

The contractor shall establish appropriate divisions of responsibilities and separations of duties as needed to eliminate conflicts of interest.

Whenever there are multiple contractors performing information technology support, the contractor shall develop and maintain a roster showing the roles and responsibilities for maintaining the information and the information system, ensuring there are checks and balances in place for all IT processes.

11.6 AC-6 Least Privilege

The contractor shall ensure that employees have access to only those rights required to perform their specific duties. The user rights shall be controlled using the information system tools of that information system or IT asset.

In situations where data entry work is being performed, including collecting survey feedback, remittance processing, credit card processing, or other similar roles, workstations shall be configured to restrict access to information and data. At a minimum, the following activities, privileges, or handling and processes shall be restricted:

- Administrative tools, including Event viewer, and information system utilities.
- Command line access.
- Ability to install software, including adding, removing, or modifying software, unless this is part of the job responsibilities.
- File Transfer Protocol (FTP) or Telnet, (while FTP is a telecommunication issue, this shall be restricted in terms of least privilege as well).
- Local administrator rights on workstations.
- Backup rights to either the information system and/or server.
- Elevated access rights to the database software.
- Access to saving files to either an electronic, optical, or other removable media including floppy devices or Universal Serial Bus (USB) devices.

Additionally, all returns and return information and other SBU information shall be physically or logically partitioned within the information system and/or the IT environment of the contractor site, as appropriate, to ensure this sensitive information is not commingled with the information of any other party or entity, and is accessible only to authorized personnel. Partitioning can be accomplished with the use of routers & firewalls, and partitioned directories, controlled by user permissions.

Control Enhancements:

- The contractor shall explicitly authorize access per IT asset defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information.
- The contractor shall require that users of IT asset accounts, or roles, with access to Security Functions including but not limited to establishing information system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, use non-privileged accounts, or roles, when accessing non-security other information system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions. The contractor shall restrict privileged accounts on IT assets**,** applications, and databases to only those personnel who require access to perform job functions.
- All actions performed on the system using privileged roles shall be audited to deter, detect, and report on potential misuse.
- The configuration of the IT environment shall be controlled so that non-privileged users cannot access and/or perform privileged roles. As an example, a user should not be able to access the administrator functions of the IT environment.

11.7 AC-7 Unsuccessful Login Attempts

All IT assets must be configured to enforce a limit of three (3) consecutive invalid logon attempts by a user. Upon a third unsuccessful logon attempt, in a 120-minute period, the user's account shall be automatically locked. The account is to remain locked for 15 minutes or until unlocked by an information system administrator or authorized person (or password reset program).

11.8 AC-8 System Use Notification

For publicly accessible applications or web hosting environments requiring user registration, the application or hosting environment shall (i) display the information system use information when appropriate, before granting further access; (ii) display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such information systems that generally prohibit those activities; and (iii) include in the notice given to public users of the information system, a description of the authorized uses of the system.

For any information systems/applications being used, the information system or application shall display an information system usage notification (e.g., warning banner) before granting information system access. The warning banner shall state: (i) information system usage shall be monitored, recorded and subject to audit; (ii) unauthorized use of the information system is prohibited and subject to disciplinary actions, and (iii) that the use of the information system indicates consent to monitoring and recording.

11.9 AC-11 Session Lock

When a contractor uses an IT asset for IRS work, the IT asset shall be locked whenever the asset is left unattended. When a session lock is established, the information system, or application shall remain locked until the user provides appropriate identification and authentication, e.g., entering the user name and password to get access to the live session. The session lock shall also take effect whenever the information system or application is left inactive for 15 minutes.

Control Enhancement:

- When the screen lock is implemented, a generic screen saver shall be displayed in lieu of the information previously being processed.

11.10 AC-12 Session Termination

The contractor information system shall automatically terminate a user session after 30 minutes of inactivity.

11.11 AC-14 Permitted Actions without Identification or Authentication

The contractor shall identify and document specific user actions that can be performed on the information system without identification or authentication and permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives. Examples of access without identification and authentication would be instances in which the contractor maintains a publicly accessible web site allowing users to access information on the site, without identifying themselves first.

11.12 AC-17 Remote Access

The contractor shall establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorize remote access to the information system prior to allowing such connections.

Anytime a contractor allows an employee or IT support employees to remotely access the contractor's IT environment that houses and/or processes IRS SBU data, the connection must be secured using a Virtual Private Network (VPN) using two-factor authentication and FIPS 140-2 or later validated encryption. NIST identifies a VPN as an internal network connection. The use of two-factor authentication requires the use of: 1) something they know, such as a password and 2) something they possess, such as a token card, to access the information system. A representation of two-factor authentication is the use of an Automated Teller Machine (ATM) card to obtain bank access. All remote access to the asset shall be logged and monitored for unauthorized use.

Control Enhancements:

- All remote access to the IT environment shall be monitored and controlled.
- The contractor information system must implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

- The information system shall route all remote access through a limited number of managed access control points.
- The contractor shall authorize the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

11.13 AC-18 Wireless Access

The contractor shall authorize, document, and monitor all wireless access to the information system, sufficient to allow all activities to be reconstructed. Additionally, the contractor shall create and maintain documentation that defines wireless configurations, restrictions, and other related requirements. Guides to secure wireless access implementation for this control are contained in *NIST SP 800-48 Revision 1 (Wireless Network Security for Institute of Electrical and Electronics Engineers (IEEE) 802.11a/b/g and Bluetooth) and NIST SP 800-97 (Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i)*. Wireless access shall be documented in the Security Plan submitted to and approved by the IRS.

Control Enhancement:

- The information system must protect wireless access to the information system using authentication of users and devices, and encryption using FIPS 140-2 or later compliant encryption.

11.14 AC-19 Access Control for Mobile Devices

When mobile devices are used to connect to contractor resources, automated procedures shall be developed to authorize, document, and monitor all device access to the contractor's IT assets. Information shall be sufficient to enable all activities to be recorded and analyzed, as necessary.

Contractors shall develop policies for any allowed portable and mobile devices, where these information systems contain SBU data. This includes the use of blackberry devices, cellular phones, iPhones, etc. The policies shall document the approved or disapproved use of mobile devices to connect to IT assets hosting IRS information.

For mobile devices 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. For more information see the PE controls, Section 21 Physical Security & Environmental Protections, Physical Security of Computers, Electronic, and Removable Media and section 20.4 Media Storage.

For any contractors, who are managing IT applications, the contractor shall ensure that access to external information systems is controlled.

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. For more

information see the PE controls, Section 21 Physical Security & Environmental Protections, Physical Security of Computers, Electronic, and Removable Media, and Removable Media.

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

Control Enhancements:

- 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 FIPS 140-2 or later, Security Requirements for Cryptographic Modules. Servers are not mobile computer devices. Non-business personally-owned information systems shall never be used to handle IRS information.

11.15 AC-20 Use of External Information Systems

External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness.

The contractor shall ensure that only those IT assets identified for processing of IRS information shall be used in conducting IRS work. For purposes of this document, any IT assets not identified to the IRS as being in the scope of IRS work are considered external information systems. The contractor shall not use other external information systems within their home or business for the purpose of conducting IRS work.

If external information systems are required, trust relationships shall be established both logically and in writing. In addition, these external components shall be identified to the IRS.

Only IT assets that have been identified and authorized for IRS contract work can be used to handle or process IRS information. Privately owned (non-business) information systems, (e.g., family owned information systems) shall not be authorized or used to handle or process IRS information or work.

Control Enhancements:

- The contractor shall permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

(a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan.
(b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system. The contractor shall limit the use of organization-controlled portable storage devices media by authorized individuals on external information systems.

11.16 AC-21 Information Sharing

The contractor shall facilitate information sharing, as allowed by the IRS or contract, by identifying the appropriate personnel who review and determine if the information being shared with a partner organization matches the contractor access requirements for the information being shared.

a. The contractor shall employ automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.

Note: This requirement applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment.

11.17 AC-22 Publicly Accessible Content

The contractor shall designate individuals authorized to post information onto a publicly accessible information system as allowed by the IRS or contract; and train authorized individuals to ensure that publicly accessible information does not contain non-public information and to maintain the integrity of information of the web site. The contractor shall:

a. Designate individuals authorized to post information onto a publicly accessible information system.
b. Train authorized individuals to ensure that publicly accessible information does not contain non-public IRS information.
c. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that non-public information is not included.
d. Review the content of publicly accessible information for non-public information at a minimum quarterly and remove such information if discovered.

12 Awareness and Training (AT)

The IRS has established policies and procedures to ensure awareness and training take place at contractor sites.

12.1 AT-1 Security Awareness and Training Policy and Procedures

The contractor shall develop, document, disseminate, and review/update policies and procedures annually within the FISMA calendar (July 1 - June 30) or if there is a significant change to security awareness and training, as these relate to IRS work.

The contractor shall ensure all contractor and subcontractor employees who require access to IRS information or information systems, regardless of their physical location, complete the required Security Awareness Training. This also applies to contractors and subcontractors working at contractor-managed facilities using contractor-managed IT assets. IRS will provide the required training to contractors.

12.2 AT-2 Security Awareness Training

For each contractor and subcontractor employee assigned to a contract/order, the contractor shall submit confirmation of completed Security Awareness Training (using the form at the Mandatory Briefing web site or upon email request to CSM at awss.csm.training@irs.gov), via email, to the COR and the CSM upon completion not later than ten (10) business days of starting work on the immediate contract/order.

Thereafter, each contractor and subcontractor employee assigned to the contract/order shall complete Security Awareness Training annually. The contractor shall submit confirmation of completed annual Security Awareness Training on all contractor and subcontractor employees assigned to this contract/order, via email, to the CO, COR, and the CSM upon completion or as requested by CSM (whichever date is earlier).

It is the responsibility of the contractor to ensure all briefing materials have been received, and distributed to contractor and subcontractor employees. This includes all active employees and subcontractors who provide support to the IRS contract, who are located remotely or on-site. The contractor is responsible for providing the list of all employees, who have completed training to the IRS. This briefing may be obtained by contacting awss.csm.training@irs.gov .

Control Enhancement:

The contractor shall include security awareness training on recognizing and reporting potential indicators of insider threat.

12.3 AT-3 Role Based Security Training

Any contractor or subcontractor employee who has a significant IT security role or responsibility shall complete specialized IT security training pertinent to the role/responsibility. This includes any contractor or subcontractor employee with a privileged network user account that allows full system permission to resources within their authority or to delegate that authority. A list of the specialized IT security roles and the number of hours of training required for each role may be obtained by contacting awss.csm.training@irs.gov.

Contractor and subcontractor employees newly assigned to a significant IT security role, including at time of contract award, must complete the training prior to commencement

of work. Proof of specialized IT training is required within 10 business days at the start of work in the specialized IT security role and annually, thereafter.

Existing contracts that have been modified or will be modified to include contractor and subcontractor employees identified as having a specialized IT security role must complete the Specialized IT security training within 45 days of the contract modification designating an employee to a specialized IT security role and annually, thereafter.

12.4 AT-4 Security Training Records

The contractor shall provide all security training records to the COR and to awss.csm.training@irs.gov.

13 Audit and Accountability (AU)

For all contractors, where more than one (1) employee is allowed to access an IT asset, including servers, workstations, laptops, etc., the contractor shall enable auditing on those assets to ensure that actions shall be logged, and so that access to IRS information shall be deterred, detected, monitored, and tracked.

13.1 AU-1 Audit & Accountability Policy and Procedures

Contractors shall develop, document, disseminate audit and accountability policies and procedures; and review/update those policies and procedures at least annually or if there is significant change that define how auditing shall take place for the contractor site. The policies and procedures shall be sufficient to enable monitoring of IT assets.

13.2 AU-2 Auditable Events

At contractor sites, auditing shall be accomplished to record and monitor access to IT assets, including, but not limited to access to: routers, operating information systems, databases, remote access, and application programs. Audit records shall be sufficient to enable re-creation of information system related events.

The contractor shall identify and enable auditable events that shall allow the contractor to detect, deter, and report on suspicious activities. The required auditable events are listed in the table below.

Table 3: Auditable Events

#	Auditable Events
1	Log onto system
2	Log off of system
3	Change of Password
4	All system administrator (SA) commands, while logged on as an SA
5	Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS) (Not Applicable for Windows based systems)

6	Creation or modification of superuser groups
7	Sub-set of security administrator commands, while logged on in the security administrator role
8	Sub-set of system administrator commands, while logged on in the user role
9	Clearing of the audit log file
10	Startup and shut down of audit functions
11	Use of identification and authentication mechanisms (e.g., user id and password)
12	Change of file or user permissions or privileges (use of suid/guid, chown, su, etc.) (Not Applicable for Windows based systems)
13	Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system.
14	Changes made to an application or database by a batch file.
15	Application critical record changes
16	Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility)
17	All system and data interactions concerning Taxpayer Data

Control Enhancement:
The contractor shall review and update the list of auditable events every two (2) years.

13.3 AU-3 Content of Audit Records

The information system shall generate audit records containing enough detail to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected in the audit records for audit events identified by type, location, or subject.

Examples of content that may satisfy this requirement are: time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

At a minimum, information systems shall generate audit records containing information that establishes:

- What type of event occurred
- When the event occurred
- Where the event occurred
- The source of the event

- The outcome of the event
- The identity of any individuals or subjects associated with the event

13.4 AU-4 Audit Storage Capacity

Audit records shall be stored in off line storage, but shall be able to be retrieved and used, as necessary. Storage capacity shall be sufficient to enable storage management and retrieval of auditable events.

Audit record storage capacity shall be allocated based on the types of auditing to be performed and the audit processing requirements, in accordance with IRS defined audit record storage requirements.

13.5 AU-5 Response to Audit Processing Failures

In the event that the audit records become full and/or auditing stops recording, the information system shall be configured so that an alert is generated, and appropriate management is notified to take action to ensure audit records are retained and the information system is returned to normal operations. The contractor shall develop and implement an action plan that can be used in an audit processing failure.

13.6 AU-6 Audit Review, Analysis, and Reporting

Automated reports shall be generated, and management or designated personnel shall review reports to identify unusual activity and take action, as necessary. The contractor shall document the timeframe for when they shall be conducting reviews.

For any compromise to IRS SBU information, this shall be identified as an information security incident, and reported to the *IRS Situation Awareness Management Center* at (866) 216-4809**.** See procedures in Incident Response and Incident Reporting section of this document.

Control Enhancement:

- The contractor shall employ automated mechanisms to integrate audit review, analysis, and reporting processes to support contractor processes for investigation and response to suspicious activities.
- The contractor shall analyze and correlate audit records across different repositories to gain contractor-wide situational awareness.

13.7 AU-7 Audit Reduction and Report Generation

The information system shall provide an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents. This capability shall not alter the original content or time ordering of audit records.

Audit reports shall be developed, using a user readable format to enable a manager or designated official to readily identify significant events. These events shall be reviewed for unusual activities, suspicious activities or suspected violations, using after-the-fact auditing techniques.

Control Enhancement:

- The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.

13.8 AU-8 Time Stamps

All audit records will contain a timestamp. Internal system clocks will generate the timestamp. Record timestamps can be mapped to Coordinated Universal Time (UTC), Greenwich Mean Time (GMT), or Local time with an offset from UTC.

Control Enhancement:

The information system compares synchronized internal information system clocks at least quarterly with an authoritative time source.

13.9 AU-9 Protection of Audit Information

The contractor shall identify all individuals who are responsible for reviewing audit information. Access rights shall be restricted so that only authorized audit review employees have access to this information. The management and retention of all audit information must remain in control of the contractor identified in the IRS contract and safeguarded as SBU information. Audit logs shall be protected by strong access controls to help prevent unauthorized access to ensure events are not modified or deleted. To ensure separation of duties, where possible, management of the audit logs should be an individual other than system administrator.

Control Enhancement:

(1) The information system shall protect audit information and tools from unauthorized access, modification or deletion.

(2) Access to on-line audit logs shall be strictly controlled.

(3) Audit logs shall be protected by strong access controls (i.e. the AC control family).

(4) Management of audit information shall be conducted by an approved privileged user (e.g. System Administrator)

13.10 AU-11 Audit Record Retention

Audit records must be retained for a period of seven (7) years, if there are returns or return information, for the purpose of providing support in after-the-fact investigations of security incidents. Copies shall be provided to the IRS, as necessary to investigate potential IRS impacted events. Specific retention periods are identified in the table below.

Table 4: Retention Periods

Audit Operations	LOW	MOD	HIGH	OTHER
Central Online Log Data	7 days	7 days	7 days	

Retention Period				
Offline Log Data Retention Period	At least 30 days	At least 90 days	7 years	All 6103 data kept for 7 years
Local System Log Rotation	Once a week or 28 MB in size	12 to 24 hours or 5 MB in size	Once an hour	
Transfer Periods to Central Online / Offline data repository	3 to 24 hours	15 to 60 minutes	Active or 15 minute intervals	
Analysis Requirements	Once a week	2 to 3 times a week	One a day	
Log Integrity / Encryption	No / No	Yes / No	Yes / Yes	

13.11 AU-12 Audit Generation

Auditing tools shall be in place to allow the contractor to generate reports to enable a review of audit events based upon specialized contractor needs. For example, if file directories have restricted access, a contractor shall choose to audit all accesses to that directory. As another example, the contractor shall wish to view all users who access an information system or network during non-authorized hours.

Information systems shall have the capability to generate audit records for the events and content as defined in 13.2 and 13.3. The information system shall have the capability to allow the selection of auditable events for specific information system components.

14 Security Assessment and Authorization (CA)

An assessment of security controls provides the contractor and IRS with an assurance that security controls are established and operating, as intended, within the contractor environment. Key points of this process include:

- Conducting an independent assessment to ensure the contractor-defined security controls are operating as intended,
- Identification of weaknesses/risks,
- Briefing management of weaknesses/risks,
- Formal IRS acceptance of any associated risks or mitigation of risks or implementation of compensating controls, and
- Accrediting the environment by authorizing the environment to be operational, by a senior contractor official.

Assurances shall be made to ensure security controls have been applied; that testing has been conducted to validate controls; and that a designated official has authorized the use of the IT assets, and identified any risks accepted by the contractor management.

14.1 CA-1 Security Assessment and Authorization Policies and Procedures

The contractor shall develop, document and disseminate assessment and authorization policies and procedures. The contractor shall review/update the policies and procedures annually or if there is a significant change.

14.2 CA-2 Security Assessments

The contractor shall develop a security assessment plan, and shall produce a security assessment report with the results of the assessment. This assessment shall be conducted annually or when major changes have been made to the IT environment to ensure the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the IT environment. Security assessment and audit results shall be made available to appropriate authorized personnel.

- For contractors maintaining information systems, a formal independent test shall be conducted of the entire IT environment.

Control Enhancement:

- The contractor shall employ an independent assessor or assessment team to assess the security controls in the information system to validate that the security controls are appropriately defined and the controls are operating as intended. Assessments shall include all IT assets, including, but not limited to the vendor-developed applications to support IRS operations, hosting platforms including virtualization, cloud, operating systems, relational databases, and programming languages etc. Independent assessments can be obtained from elements within the organization or can be contracted to public or private sector entities outside of the organization.

14.3 CA-3 Information System Connections

The contractor shall maintain a user authorization list that defines the external systems, individuals authorized to access the external system, and the user rights assigned to these individuals.

System to system connections are to be authorized and documented via Interconnection Security Agreements. Interconnection Security Agreements shall be reviewed and updated (if necessary) at least annually.

Control Enhancement:
The contractor, based on a risk assessment, shall employ one of the following policies for allowing contractor IT assets to connect to external information systems:

- Allow-all, deny-by-exception (blacklisting)
- Deny-all, permit-by-exception (whitelisting)

14.4 CA-5 Plan of Action and Milestones

For any security reports issued to the contractor, including internal independent reviews, the contractor is responsible for developing a POA&M that identifies corrective actions and/or mitigating controls for any identified vulnerabilities.

POA&Ms shall be provided to the COR or delegate quarterly, demonstrating progress made toward weakness remediation.

14.5 CA-6 Security Authorization

The contractor shall assign a senior-level official as the authorizing official for the information system. The assigned senior official shall authorize the information system prior to it being put into operation, document the authorization and sign the documentation as the responsible party. By authorizing an information system to operate, the senior official is accepting the risk for the information system. The senior official ensures the information systems security authorization is reviewed and updated every 3 years or when a significant impact to the information system occurs.

14.6 CA-7 Continuous Monitoring

All contractors shall establish and implement a continuous monitoring strategy that includes a configuration management process, a security impact analysis of changes to an information system, and continuous/ongoing security control assessments. When security controls are identified as non-compliant, they must be brought into compliance within a 24 hour period. At least annually, the security state of the information system shall be reported to the appointed COR, or Contracting Officer if no COR has been appointed.

The contractor shall implement a continuous monitoring strategy that includes ongoing monitoring of the security controls (e.g. monthly policy checking and vulnerability scans), in accordance with the defined configurations to identify any controls that may not be compliant.

Control Enhancement:
The contractor shall employ impartial, independent assessors or assessment teams to monitor the security controls in the information system on an ongoing basis. A Contractor Security Assessment performed by the Internal Revenue Service does not qualify as an impartial, independent assessment for this control.

14.7 CA-9 Internal System Connections

The contractor shall authorize any internal connections to IT assets processing IRS sensitive information and document the interconnection characteristics, security requirements, and the type of information transmitted between the IRS assets and other internal contractor information systems.

15 Configuration Management (CM)

Configuration management ensures that organizations are using the correct versions of procedures and processes and that there are formal mechanisms in place to implement new procedures and processes.

15.1 CM-1 Configuration Management Policy and Procedures

The contractor shall develop, document, disseminate, and review/update the Configuration Management policies and procedures annually or if there is a significant change to ensure adequate policy and procedures are developed and implemented.

15.2 CM-2 Baseline Configuration

The contractor shall develop, document, and maintain a current baseline configuration for all IT assets. This inventory shall include all databases, applications, etc. that are being used as part of the baseline configuration for servers, routers, workstations, etc.

Control Enhancements:

- The contractor shall review and update the baseline configuration of the information system:
  - (a) Annually,
  - (b) When required due to a significant change, and
  - (c) As an integral part of information system component installations and upgrades.
- The contractor shall retain older versions of baseline configurations as deemed necessary to support rollback.
- The contractor shall issue a loaner laptop with a pre-defined configuration to contracted personnel traveling to locations that are deemed to be of significant risk. Upon the individuals return, security safeguards (e.g., reimaging hard drive, examining for signs of tampering) are to be applied to the laptop.

15.3 CM-3 Configuration Change Control

The contractor shall develop and implement a change control process. This process shall ensure that all changes are approved, tested, documented, and published, using a change control log, available for review. This log shall be retained using automated tools, such as electronic spreadsheets, databases, etc.

The contractor shall develop and maintain a change management process to ensure all changes introduced into the environment are documented, reviewed for approval, and maintained using a standard operating procedure/process. Change logs will be retained for three (3) years. The contractor will audit and review activities associated with configuration-controlled changes to the information system and changes will be coordinated through a configuration change board (CCB) that meets, at a minimum, monthly.

Control Enhancement:

- The contractor shall test, validate, and document changes to the information system before implementing the changes on the operational information system.

15.4 CM-4 Security Impact Analysis

When contractors are involved in application or information system development, the contractor shall develop a process to assess all information system or application changes to determine if there is any impact to the security controls that shall be created by the change.

15.5 CM-5 Access Restrictions for Change

The contractor shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

15.6 CM-6 Configuration Settings

The contractor shall establish and document configuration settings for information technology products employed within the information system using security configuration tools. At a minimum, the following security configuration tools should be utilized.

At a minimum, the assessment shall include one (1) of the following for each IT asset category:

Table 5: Security Configuration Tools

IT Asset	Assessment Tool	Source
Workstations & Laptops	NIST Approved Security Content Automation Protocol (SCAP) Tool	http://nvd.nist.gov/scapproducts.cfm (NIST Link)
	Vendor Supplied Compliance Checker i.e. Microsoft Security Baseline Analyzer	http://www.microsoft.com/en-us/download/details.aspx?id=7558 (Microsoft Link)
	Windows Policy Checker Found in the Windows-SCAP folder	IRS Contractor Security Assessments
Servers (Local Area Network (LAN), Wide Area Network (WAN), Domain Name Server (DNS), etc.)	NIST Approved SCAP Tool	https://nvd.nist.gov/scapproducts.cfm (NIST Link)
	Vendor Supplied Compliance Checker i.e. Microsoft Security Baseline Analyzer	http://www.microsoft.com/en-us/download/details.aspx?id=7558 (Microsoft Link)
	Windows Policy Checker	IRS Contractor

IT Asset	Assessment Tool	Source
	Found in the appropriate folder for Windows OS or UNIX	Security Assessments
Switches & Routers	Vendor Supplied Tools i.e. Nipper – Network Device Security Audit Tool	http://www.itsyourip.com/networking/nipper-network-device-security-audit-tool/
	Cisco Security Analyzer Found in the Cisco Folder	IRS Contractor Security Assessments

The contractor shall implement the configuration settings.

Any deviations from established configuration settings for information system components shall be identified, documented, and approved based on operational requirements. Changes to the configuration settings shall be monitored and controlled in accordance with defined configuration change management policies and procedures.

The contractor shall document all deviations from the standard security controls and ensure these are brought into compliance using a standard configuration process.

15.7 CM-7 Least Functionality

All IT assets shall be restricted to ensure that least functionality is implemented to restrict the information system to only essential ports, protocols and services. Employees performing data entry would not require Information System Administrator or elevated privileges.

Protocols, Services and Logical Ports that shall be restricted include but are not limited to FTP, Telnet, Structured Query Language (SQL) services enabled on non-SQL servers, and USB ports. In addition, the contractor shall review the information system at a minimum annually to identify and eliminate unnecessary functions, ports, protocols, and/or services. The contractor shall ensure compliance with all defined requirements related to functions, ports, protocols, and services.

The contractor shall identify all programs authorized to be used in the IT environment. This list must be updated as changes are made and reviewed at least annually to ensure the list is current. The contractor shall also define those programs not authorized to be used in the IT environment. By default, the contractor shall maintain the most restrictive permissions and use of programs.

Control Enhancements:

- The contractor shall review the information system at least annually to identify and disable unnecessary functions, ports, protocols, and/or services.

- The information system shall prevent unauthorized software from being executed.
- The contractor shall identify all programs unauthorized to be used on the information system. An “allow-all, deny-by-exception” policy shall be employed to prohibit the execution of unauthorized programs. The list of unauthorized programs shall be reviewed and updated at a minimum annually.

15.8 CM-8 Information System Component Inventory

The contractor shall develop, document, and maintain an inventory of all hardware, software, and removable media that accurately reflects the current information and includes all components within the authorization boundary of the information system to support IRS work. The inventory shall include inventory serial number, description of the inventory item, owner of the inventory item, date placed in inventory, and date inventory was validated. At a minimum, the inventory shall be reviewed and reconciled annually. Inventory shall be sufficient to enable recovery of IT assets that are identified as lost, stolen, or disclosed.

Control Enhancements:

- The contractor shall update the inventory of information system components as an integral part of component installations, removals, and information system updates.
- The contractor shall:
  (a) Employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
  (b) Take the following action when unauthorized components are detected:
    - disable network access by such components,
    - isolate the components, and
    - notify appropriate officials.

- The contractor shall verify that all components within the authorization boundary of the information system are either inventoried as a part of the information system or recognized by another information system as a component within that information system. Inventory duplication is to be resolved so a component is only inventoried as part of one information system.

15.9 CM-9 Configuration Management Plan

The contractor shall develop, document, and implement a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures. A process shall be established for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items. Configuration items for the information system shall be defined and configuration items shall be placed under configuration management. The configuration management plan shall be protected from unauthorized disclosure and modification.

At a minimum, the contractor shall define all items being managed under the configuration plan, manage the configuration plan as well as the configuration items, and protect the configuration management plan from unauthorized disclosure and/or modification.

15.10 CM-10 Software Usage Restrictions

The contractor shall use software and associated documentation in accordance with contract agreements and copyright laws; track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

15.11 CM-11 User-Installed Software

The contractor shall establish and enforce a policy governing the installation of software by users. Compliance with the policy shall be monitored, at least annually.
The contractor shall develop and manage a process to apply all software changes to the environment. Software must be routinely monitored, at least monthly to ensure that the approved software is operational and that no other software has been introduced into the environment.

16 Contingency Planning (CP)

All contractors shall develop a contingency plan and business resumption plan to provide information for how the contractor shall restore business operations and resume business in the event of failed IT assets or the inability to access the facility.

16.1 CP-1 Contingency Planning Policy and Procedures

All contractors shall develop, document, disseminate, and review/update policy and procedures, annually or if there is a significant change, that define the company requirements that shall be addressed in terms of IT Contingency Planning. The policies and procedures shall be sufficient to address the planning elements required for a particular contractor site. Policies and procedures shall address the need to identify essential business functions supported, provide restoration priorities and identify contingency roles and responsibilities.

16.2 CP-2 Contingency Plan

All contractors shall develop Contingency Plans (CP) to address IT and Physical Security planning. These shall identify key business functions provided to the IRS, alternate work sites, alternate resources, contact information, and identify the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). The plans shall document the activities associated with restoring all IT assets, including information systems, and applications after a disruption or failure.

As part of the CP, an Occupant Emergency Plan (OEP) shall be included to address occupant safety and security procedures, in the event of an emergency. The OEP should be shared with all employees who have work related to the IRS contract or any impacted employees. At least annually, the plan shall be reviewed and updated and the

contractor shall conduct OEP drills, documenting the results and incorporating lessons learned into the OEP. Additionally, as part of the CP the contractor shall develop and include a Business Impact Analysis (BIA). The BIA will be reviewed and updated annually.

The contractor shall distribute copies of the contingency plan to key personnel who are responsible for implementing the contingency plan ensuring updates are communicated. A copy of the plan will also be provided to key IRS stakeholders including the CO and COR.

The CP is considered SBU information and shall be protected from unauthorized disclosure and modification.

Control Enhancement:

- The contractor shall coordinate contingency plan development with contractor elements responsible for related plans.
- The contractor shall plan for the resumption of essential missions and business functions within a specified period of time upon contingency plan activation.
- The contractor shall identify critical information system assets supporting essential missions and business functions.

16.3 CP-3 Contingency Training

The contractor shall train personnel in their contingency roles and responsibilities within 30 days of assuming a contingency role or responsibility, when changes to the information are sufficient to warrant the training, and provide refresher training at least annually.

16.4 CP-4 Contingency Plan Testing and Exercises

All Contingency Plans shall be tested at least annually. For all IRS FISMA-reportable information systems, the IRS shall develop and implement a test plan. The contractor shall develop and test a plan to ensure that operations can be restored. The contractor shall review the contingency plan results and initiate corrective actions, if needed. Plan testing and exercises shall include a tabletop exercise and functional testing. A copy of the testing results should be provided to the IRS along with any documentation and corrective actions to be taken.

Control Enhancement:

- The contractor shall coordinate contingency plan testing and/or exercises with contractor elements responsible for related plans.

16.5 CP-6 Alternate Storage Site

The contractor shall establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information/ media/data. All backup information/media/data containing SBU information shall be encrypted. The alternate storage site shall be geographically separated from the contractor site to enable recovery of operations and shall provide information security safeguards equivalent to that of the primary site.

Control Enhancements:

- The contractor shall identify an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.
- The contractor shall identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

16.6 CP-7 Alternate Processing Site

The contractor shall ensure that the equipment and supplies required to resume operations at the alternate site are in place, or that required equipment/supplies are made available within specified timeframes to avoid unacceptable delays in the delivery of contracted services. The IT, personnel, and physical security controls shall be commensurate with the sensitivity of the information being restored, and with the security of the original processing site.

The contractor shall safeguard IT assets and information at the alternate site using equivalent security controls as used at the primary site.

Control Enhancements:

- The contractor shall identify an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.
- The contractor shall identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
- The contractor shall develop alternate processing site agreements that contain priority-of-service provisions in accordance with the contractor's availability requirements.

16.7 CP-8 Telecommunications Services

The contractor shall ensure that the primary and alternate processing sites have the necessary telecommunications services needed to support the information systems, so as to resume operations within specified timeframes.

Control Enhancements:

- The contractor shall:
  (a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the contractor's availability requirements.
  (b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.
- The contractor shall obtain alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

16.8 CP-9 Information System Backup

For contractors with information systems, in order to achieve the Recovery Point Objective (RPO) and the Recovery Time Objective (RTO) of the business customer, the contractor shall back up data contained in the information systems to enable contractors to provide continuous support to IRS. The contractor shall backup information system documentation including security-related documentation. Backups include user-level information, system-level information, and SBU information. The contractor shall test backup restoration capability to ensure information could be recovered, as necessary. The contractor shall protect the confidentiality, integrity, and availability of backup information at storage locations.

Control Enhancements:

- The contractor shall test backup information semi-annually to verify media reliability and information integrity.

16.9 CP-10 Information System Recovery and Reconstitution

The contractor shall ensure there are procedures in place to provide for the recovery and reconstitution of any IT assets or information system to a known state after a disruption, compromise, or failure. The contractor shall test backup restoration capability to ensure information could be recovered, as necessary. This control moves beyond table top exercises to ensure that data can be recovered from backup media, as necessary.

Control Enhancements:

- The information system implements transaction recovery for information systems that are transaction-based.

17 Identification and Authentication (IA)

Identification and authentication is a process that is used to identify an individual (e.g. user name) to the information system and authenticate (e.g. password or token) the individual, prior to allowing access to an information system, such as a workstation, laptop, server, etc.

17.1 IA-1 Identification and Authentication Policy and Procedures

The contractor shall develop policies and procedures that describe how identification and authentication shall be managed. Policies and procedures shall be developed, documented, disseminated, and reviewed/updated annually or if there is a significant change to facilitate implementing identification and authentication of security controls.

17.2 IA-2 Identification and Authentication (Organizational Users)

For access to any IT asset by contractor users (including subcontractors), the contractor shall require identification and authentication to access this asset. Typically this is known as a user name and password. Authentication shall be accomplished using standard methods such as passwords, tokens, smart cards, or biometrics.

17.3 IA-3 Device Identification and Authentication

The contractor shall ensure that information systems uniquely identify and authenticate all devices before allowing a connection to the contractor's network. Examples of devices that would be connected to the network include laptops and workstations.

Common device identifiers such as Media Access Control (MAC), Internet Protocol (IP), or device-unique token identifiers shall be used to identify machine and device names.

17.4 IA-4 Identifier Management

The contractor shall manage all identifiers, e.g. user names, for either IT systems or IT assets to include the following:

a. Establishing user accounts, only after receiving authorization from an individual assigned and authorized to approve new user accounts, user roles, groups, etc.
b. Ensuring that user groups establish a naming convention to enable management to understand the creation and management of user accounts, groups, etc. Examples of user group names would be:
    - AlphaCompanyAdminGroup
    - AlphaCompanyHelpDeskGroup
c. Ensuring that user names or similar accounts cannot be reused. This will enable auditing to be accomplished for the seven (7) year period while ensuring all activities are only associated with a single user account.
d. Ensuring that user accounts are automatically disabled after 120 days of inactivity.
e. Ensuring that privileged accounts, e.g., system administrator, are disabled after 60 days of inactivity.

17.5 IA-5 Authenticator Management

All passwords shall be complex. A strong password contains a combination of upper and lower case alphanumeric characters, numbers, and special characters. A new password shall be changed every 90 days. Passwords shall be configured so they cannot be reused for 24 consecutive password changes. Other authenticators, including tokens and certificates, shall meet requirements identified in the password management controls.

When passwords are lost, the contractor shall ensure there is a process to manage lost passwords to ensure information is not compromised. All vendor passwords or passwords issued with the information systems and applications shall be changed, including any default passwords.

Employees shall be trained on the proper handling of individual passwords to prevent unauthorized use or modification.

Control Enhancements:

- The information system, for password-based authentication:

(a) Enforces minimum password complexity. Passwords must contain a minimum of eight (8) characters and must contain a combination of letters, numbers, and special characters.
(b) Enforces at least one (1) character is changed when new passwords are created.
(c) Encrypts passwords in storage and in transmission.
(d) Enforces password minimum lifetime restrictions of one (1) day and maximum of ninety (90) days.
(e) Prohibits password reuse for 24 generations.
(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

- The information system, for Public Key Infrastructure (PKI)-based authentication:
  (a) Validates certificates by constructing a certification path with status information to an accepted trust anchor.
  (b) Enforces authorized access to the corresponding private key.
  (c) The contractor shall ensure that the IT system used to authenticate employees has a backup mechanism able to assume authentication responsibilities in a timely manner if the primary authentication device fails.
  (d) Implements local storage of revocation data to support path discovery and validation in the event that revocation data is unavailable via the primary storage location on the network.
  (e) The contractor shall require that the registration process to receive Homeland Security Presidential Directive-12 Smart Cards be carried out in person with a designated registration authority with authorization by a designated contractor official (e.g., a supervisor). Note: This only applies when contractors are also accessing IRS systems and/or facilities.
  (f) The contractor shall map the authenticated identity to the account of the individual or group.
- The information system, for hardware token-based authentication, employs mechanisms that satisfy token quality requirements.

17.6 IA-6 Authenticator Feedback

When a password or other authentication mechanism is used, the information system or application shall generate non-readable characters, such as asterisks to prevent this information from being viewed by an unauthorized individual.

17.7 IA-7 Cryptographic Module Authentication

When contractors are employing cryptographic modules for authentication, the encryption modules shall be compliant with NIST guidance (i.e., FIPS 140-2 or later). Current FIPS 140-2 validation lists can be found at http://csrc.nist.gov/groups/STM/cmvp/validation.html.

When contractors are employing cryptographic modules for Kerberos authentication, AES128_HMAC_SHA1 and AES256_HMAC_SHA1 are the only allowable encryption types.

17.8 IA-8 Identification and Authentication (Non-Contractor Users)

For any contractor who develops or manages public facing web servers, which require authentication, the contractor shall ensure that non-contractor users are uniquely identified and authenticated.

18 Incident Response (IR)

Whenever there is a compromise of IRS information, it is important to contact the IRS within one (1) hour if an incident or potential incident has been detected. The IRS shall work closely with IRS contractors to quickly respond to a suspected incident of unauthorized disclosure or inspection.

An incident is a violation or suspected violation of information security policies and practices as required by this document, and implemented by the contractor. Types of incidents include the following:

Table 6: Examples of Security Incidents

Incident Type	Description
Denial of Service	An attack that prevents or impairs the authorized use of networks, information systems, or applications by exhausting resources.
Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.
Unauthorized Access	A person or information system gains logical or physical access without permission to a network, information system, application, data, or other resource.
Inappropriate Usage	A person violates acceptable information system use policies or improper use of SBU data (e.g., IRC § 6713 and 7216).
Multiple Component	A single incident that encompasses two (2) or more incidents.
Theft	Removal of information systems, data/records on information system media or paper files.
Loss/Accident	Accidental misplacement or loss of information systems, data/records on information system media or paper files.
Disclosure of Sensitive Data	Disclosure of Sensitive Data refers to the unauthorized, inadvertent disclosure of SBU/PII data.

18.1 IR-1 Incident Response Policy and Procedures

The contractor shall develop, document, disseminate, and review/update incident response policies and procedures annually or if there is a significant change to detect and report all incidents, as these relate to IRS work.

18.2 IR-2 Incident Response Training

All contractor employees shall be trained on incident response and reporting procedures at least annually to understand their responsibilities on reporting security related incidents (unless required otherwise in the contract, this can be satisfied by completing the annual security awareness training). Training is due within 30 days of assuming an incident response role and responsibility, when required by information system changes, and annually thereafter.

18.3 IR-3 Incident Response Testing

The contractor shall annually test and/or exercise the incident response capability to determine the incident response effectiveness and document the results to ensure the policies and procedures continue to function, as intended. At a minimum, testing shall ensure that the reporting phone numbers identified in contractor procedures are accurate. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises.

Control Enhancement:
The contractor shall employ automated mechanism to more thoroughly and effectively test incident response capability.

18.4 IR-4 Incident Handling

The contractor shall implement an incident handling capability for security incidents that includes a procedure describing the process that shall be used in the event an incident is detected. Incident handling procedures shall document the process used to handle incidents, including preparation, detection and analysis, containment, eradication, and recovery. Incident handling activities shall be coordinated with contingency planning activities. Lessons learned from ongoing incident handling activities shall be incorporated into incident response procedures, training, and testing/exercises, and shall implement the resulting changes accordingly.

Contractors shall routinely track and document security incidents potentially affecting the confidentiality of SBU data. Where contractors rely on IT technical support, the contractors shall ensure the IT support teams address the need to manage and track incidents.

Control Enhancement:

- The contractor shall coordinate incident response testing with contractor elements responsible for related plans.

18.5 IR-5 Incident Monitoring

The contractor shall track and document all information system security incidents. Examples include maintaining records about each incident, the status of the incident, and other pertinent information needed for forensics, evaluating incident details, and trend analysis.

For companies using a limited number of IT assets, the contractor shall ensure that security software is installed that shall allow potential incidents to be contained and information retained about the potential incident.

18.6 IR-6 Incident Reporting

All incidents related to IRS processing, information or information systems shall be reported within one (1) hour to the CO, COR, and SAMC. Contact the *SAMC* via telephone at (866) 216-4809 (TTY 800-877-8339).

Control Enhancement:

- The contractor shall employ automated mechanisms to assist in the reporting of security incidents.

18.7 IR-7 Incident Response Assistance

All contractors shall have an individual (or help desk or incident response team) identified who shall provide assistance on the handling of potential security incidents. This support individual shall have adequate training and understanding to help a contractor resume business, while providing support to contain and manage a potential security incident.

Control Enhancement:

- The contractor shall employ automated mechanisms to increase the availability of incident response-related information and support.

18.8 IR-8 Incident Response Plan

The contractor shall develop and annually review an incident response plan that provides the high-level approach to handle incidents. The plans shall:

- Provide the organization with a roadmap for implementing its incident response capability;
- Describe the structure and organization of the incident response capability;
- Provide a high-level approach for how the incident response capability fits into the overall organization;
- Meet the unique requirements of the organization, which relate to mission, size, structure, and functions;
- Define reportable incidents;
- Provide metrics for measuring the incident response capability within the organization;
- Define the resources and management support needed to effectively maintain and mature an incident response capability; and
- Is reviewed and approved by the Contractor Security Representative.

The content of the plan shall be sufficient to enable handling and reporting of security incidents within that organization.

19 Maintenance (MA)

Maintenance ensures that all IT assets are able to be used and ensures the integrity and reliability of the equipment. All contractors, small and large, shall rely on the operation and functionality of equipment if they are to provide continued service to the IRS.

19.1 MA-1 System Maintenance Policy and Procedures

The contractor shall develop, document, disseminate, and review/update policies and procedures annually or if there is a significant change describing maintenance procedures to be used for that contractor site.

19.2 MA-2 Controlled Maintenance

The contractor shall establish a formalized information systems maintenance program that applies to all types of maintenance to any system component (including applications, scanners, copiers, and printers) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement).

The contractor shall schedule, perform, document and review records of maintenance and repairs on information systems components in accordance with manufacturer or vendor specifications and/or organizational requirements.

The contractor shall maintain a log of all maintenance to include, at a minimum:

- Date and time of maintenance
- Name of individuals or group performing the maintenance
- Name of escort, if necessary
- Description of the maintenance performed
- Information system components/equipment removed or replaced (including identification numbers, serial numbers, and/or barcodes, if applicable).

The contractor shall approve and monitor all maintenance activities, whether activities are performed, or the equipment is serviced, on site, remotely or removed to another location.

When off-site maintenance or repairs are required, the Contractor Security Representative (CSR) will explicitly approve, with an approval letter or form, the removal of the information system or system component from the contractor’s facilities. The contractor shall sanitize equipment to remove all information from associated media prior to removal from the contractor’s facilities. Any equipment that cannot be sanitized must be destroyed using media disposal processes contained in this document.

When maintenance or repair actions are completed, on site or off-site, the contractor shall check all potentially impacted security controls to verity the controls are still functioning properly.

The contractor shall ensure that all media that cannot be repaired is appropriately destroyed to minimize the inventory of malfunctioning IT assets that could potentially be lost and/or stolen.

19.3 MA-3 Maintenance Tools

When information systems environments are being used, contractor personnel shall develop, and maintain an inventory of allowed maintenance tools (software, hardware, and firmware) for that environment.

Maintenance tools shall be checked for malicious code before installation on information system(s). Maintenance security controls include identifying and monitoring a list of maintenance tools including remote maintenance tools. Maintenance equipment/tools with storage capabilities shall be properly sanitized prior to removal from the contractor site.

Control Enhancements:

- The contractor shall inspect all the maintenance tools carried into a facility by maintenance personnel for obvious improper or unauthorized modifications.
- The contractor shall check all media containing diagnostic and test programs for malicious code before the media are used in the information system.

19.4 MA-4 Non-Local Maintenance

Non-local maintenance and diagnostic activities are those activities conducted by an individual who is communicating through a network, using a broadband communication link, Virtual Private Network (VPN), or other communication path to access the contractor's IT assets.

When non-local maintenance is performed, the following shall be accomplished:

- support personnel providing non-local maintenance shall create and maintain a log that shall identify all non-local access and maintenance into a contractor's information system and
- the IT provider shall document and identify all tools used to provide maintenance support and
- the IT support shall use strong identification and authentication techniques, such as two-factor authentication or PKI. All network communications shall be terminated when work is completed.

For contractor personnel providing internal IT support, non-local maintenance shall be documented and periodically reviewed by the contractor.

Control Enhancements:

- The contractor shall document, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.

19.5 MA-5 Maintenance Personnel

The contractor shall establish a process for authorizing maintenance personnel and maintaining a list of authorized maintenance organizations or personnel. Non-escorted personnel performing maintenance on the information system shall have required access authorizations. The contractor shall designate key personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

19.6 MA-6 Timely Maintenance

The contractor shall define a list of any required spare parts and components to support maintenance and procure these as necessary. In addition, the contractor shall identify timeframes required for correcting the information system in the event of an information system failure.

20 Media Protection (MP)

Media protection controls ensure that all removable media is adequately secured to allow for the deterrence, detection, reporting, and management in the event of loss, theft, or destruction. An inventory should be maintained and provided to the IRS, upon request, that identifies all media used to store, maintain, or process SBU information. Any media that is used to store, maintain, or process IRS information cannot be commingled with non IRS data. All IRS information being handled or processed by the contractor shall be segregated from other work being performed either logically and/or physically.

Note: See Section 29.1 Destruction or return of SBU Information for sanitation and destruction of media containing SBU Information.

20.1 MP-1 Media Protection Policy and Procedures

The contractor shall develop, document, and disseminate media protection policies and procedures and review/update them annually or if there is a significant change.

The policies and procedures shall describe requirements to restrict access to information system media to authorized individuals, when this media contains IRS SBU information. Information system digital media includes but shall not be limited to diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs.

Return or Sanitization/Destruction of Hard and Softcopy Media at End of Performance under the Contract

Within three (3) months prior to the end of the base year of a contract, the contractor shall submit to the COR a plan for the return of all hard and softcopy media (identified below) or for the destruction and/or sanitization of all hard and softcopy media used, purchased specifically by the contractor for performance under the contract, or provided by the Government to the contractor for use in the performance of this contract. Examples of media that must be returned or will require sanitization and/or destruction include:

- Backups,
- Voice over Internet Protocol (VoIP),
- Hard drives,
- Routers and,
- Network - restored to original settings
- Faxes/copiers

The plan must address the time period by which the return of the property will be completed and/or how and when the destruction/sanitization will take place. The contractor may treat different property differently. The COR, in consultation with Cybersecurity, will review the plan and inform the contractor within thirty (30) days of receipt of the plan which option is preferable. The objective of this requirement is to ensure that all sensitive but unclassified, confidential, or personal data and information is no longer available to the contractor, its employees, or anyone else not authorized access to the data is able to access it. The Government has the option to perform a site visit or engage in other surveillance methods to ascertain the sanitization or destruction process. The COR may also require certification.

20.2 MP-2 Media Access

The contractor shall ensure that media access is restricted to prevent hard copy media from being lost, stolen, or disclosed. In addition, electronic, optical, and other digitally maintained media shall be restricted to prevent unauthorized access.

Employees must also be made aware of the need to protect and properly secure SBU information against inadvertent disclosure when visitors/maintenance/vendors etc., are in work area.

An after-hours walk-through shall be conducted periodically, at least quarterly, to ensure data is safeguarded after hours.

20.3 MP-3 Media Marking

For all IT assets, the contractor shall label all media to readily identify this as IRS provided information, requiring protection. Media shall be labeled “IRS Data – Sensitive But Unclassified”.

20.4 MP-4 Media Storage

For contractors who maintain IRS information, the contractor shall physically control and securely store information system media within controlled areas. When this media contains IRS SBU information, the contractor shall maintain information in a lockable metal filing cabinet. When larger volumes of information are being maintained at a contractor site, the contractor shall use automated mechanisms (key card access, biometric access, cipher locks, etc.) to restrict access to media storage areas, and to audit access attempts and access granted.

The contractor shall employ FIPS 140-2 or later compliant cryptographic mechanisms to protect information in storage. 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. For more information see the PE controls, section 21 Physical Security & Environmental Protections, Physical Security of Computers, Electronic, and Removable Media.

In addition, for all networked computers, ensure all disk areas for all computers containing SBU information are encrypted (e.g., by using an Encrypted File System) or a similar utility to encrypt data.

20.5 MP-5 Media Transport

The contractor shall document all activities associated with the transport of IT media. The contractor shall protect and control digital media during transport outside of controlled areas.

All vehicles used to transport media and paper must be secured to ensure contents cannot be inadvertently removed or lost from the vehicle, e.g. secured cabs on the back of a truck.

SBU data in hotels should be stored in locked room safe or in hotel safe in hotel management offices. Suitcases and briefcases are prone to easy theft.

Control Enhancement:

- Information systems shall implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. This applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers).

20.6 MP-6 Media Sanitization

The contractor shall sanitize information, digital, optic, and paper, prior to disposal or release for reuse. Optical mass storage media, including compact disks (CD), Compact Disc–Rewritable (CD-RW), Compact Disc Recordable (CD-R), and Compact Disc Read Only Memory (CD-ROM)), optical disks (DVD) and magnetic-optic (MO) disks shall be destroyed by pulverizing, cross-cut shredding or burning. Office shredders must cross cut shred producing particles that are no more than 1 x 5 millimeters in size. Destruction of media shall be conducted only by trained authorized personnel. Safety, hazmat, and special disposition needs shall be identified and addressed prior to conducting any media destruction. NIST SP 800-88, Guidelines for Media Sanitization contains supplemental information for media disposal.

A log shall be maintained to provide a record of media destroyed. The log shall include:

- the date of destruction;
- content of media;
- identifying serial number;

- type of media (CD, cartridge, etc.);
- media destruction performed;
- personnel performing the destruction;
- and witnesses to the destruction.

SBU media and paper material, which is identified for destruction, shall be secured sufficiently so that it is not mistaken for recycling material or general refuse.
The contractor shall demonstrate that tools and/or contract support is available to provide for sanitizing, degaussing, shredding, or other data destruction methods, sufficient to meet IRS requirements.

Any contractor authorized to perform destruction of IRS paper SBU information shall retain an IRS background check or be under escort of an employee who has a background check.

20.7 MP-7 Media Use

The contractor shall restrict the usage of writeable removable media; prohibit the usage of personally-owned equipment, software, or media to process, access, or store sensitive information; and prohibit connecting privately-owned Portable Electronic Devices (PED) or removable media to a government owned information system used to process, store, or transmit IRS information on information systems or system components using IRS SBU.

Control Enhancement:

- The contractor shall prohibit the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

21 Physical and Environmental Protection (PE)

Physical security shall be provided for a document, an item, or an area in a number of ways. These include, but are not limited to locked containers of various types, vaults, locked rooms, locked rooms that have reinforced perimeters, locked buildings, guards, electronic security information systems, fences, identification information systems, and control measures. How the required security is provided depends on the facility, the function of the activity, how the activity is organized, and what equipment is available. Proper planning and organization shall enhance the security while balancing the costs.

The IRS has categorized SBU information as moderate risk. The controls are intended to protect the information and information systems that contain SBU information. It is not the intent of the IRS to mandate requirements to those information systems and/or areas that are not handling and processing SBU information.

The Minimum Protection Standards (MPS) establish a uniform method of protecting information and items that require protecting. These standards contain minimum standards that shall be applied on a case-by-case basis. Since local factors shall require additional security measures, management shall analyze local circumstances to determine space, container, and other security needs at individual facilities. The MPS

have been designed to provide management with a basic framework of minimum security requirements.

Care shall be taken to deny unauthorized access to areas containing SBU information during duty and non-duty hours. This can be accomplished by creating restricted areas, security rooms, or locked rooms. Additionally, SBU information in any form (information system printout, photocopies, tapes, notes, etc.) shall be protected during non-duty hours. This can be done through a combination of methods: secured or locked perimeter, secured area, or containerization.

The objective of MPS standards is to prevent unauthorized access to SBU information. MPS requires (2) barriers to access SBU information under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Locked means an area or container that has a lock, and the keys or combinations is controlled. A security container is a lockable metal container with a resistance to forced penetration, with a security lock and keys or combinations which are controlled. The two (2) barriers provide an additional layer of protection to deter, delay, or detect surreptitious entry. Protected information shall be containerized in areas where other than authorized employees shall have access after-hours.

Using a common situation as an example, often an organization desires or requires that security personnel or custodial service workers have access to locked buildings and rooms. This shall be permitted as long as there is a second barrier to prevent access to SBU information. A security guard shall have access to a locked building or a locked room if SBU information is in a locked container. If SBU information is in a locked room, but not in a locked container, the guard or janitor shall have a key to the building but not the room.

There are specific items and locations that must have special attention, as described in the next few paragraphs:

Facsimile Machines (FAX)

Generally, the telecommunication lines used to send fax transmissions are not secure. To reduce the threat of intrusion, observe the following:

- Have a trusted staff member at both the sending and receiving fax machines.
- Accurately maintain broadcast lists and other preset numbers of frequent recipients of SBU information. Place fax machines in a secured area.
- Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes a notification of the sensitivity of the information and the need for protection.
- For all fax notices, the fax shall display a notice for unintended recipients to telephone the sender, to return, if necessary, and to report the disclosure and confirm destruction of the information.
- Fax servers require similar protections as other hosting server hardware.

Equipment (Corporate)

Only IRS or contractor-owned business information systems, media, and software shall be used to handle and process, access, and store SBU information. IT information systems and media shall be committed to or configured to restrict access to SBU information. The contractor shall retain ownership and control for all hardware, software, and telecommunications equipment used to handle and process, access and store SBU information.

Physical Security of Computers, Electronic, and Removable Media

Because of the vast amount of information systems, electronic, optical and other removable media store and handle and process, the physical security and control of information systems and electronic, optical or other removable media also shall be addressed. Whenever possible, information system operations shall 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 shall be met, such as keeping SBU information locked up when not in use. Removable media also shall be labeled SBU information when they contain such information. Removable media also must be encrypted and labeled SBU information when it contains such information.

In instances where encryption is not used, the contractor shall ensure that all wiring, conduits, and cabling are within the control of contractor personnel and that access to routers and network monitors are strictly controlled.

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.

Good security practice requires that inventory records of electronic, optical and other removable media be maintained for control and accountability.

Restricting Access

To assist with this requirement, SBU information shall be clearly labeled as SBU information and handled in such a manner that it does not become misplaced or available to unauthorized personnel. Additionally, warning banners advising of protecting requirements shall be used for information system screens.

Additional controls have been integrated into this document that map to guidance received from NIST. These are identified in *NIST Moderate Risk Controls for Federal Information Systems.*

The following chart illustrates the Minimum Protection Standards:

Protection Alternative Chart

Table 7: Protection Alternative Chart

Alternative Types	Perimeter Type	Interior Area Type	Container Type
Alternate #1	Secured		Locked
Alternate #2	Locked	Secured	
Alternate #3	Locked		Secured

21.1 PE-1 Physical and Environmental Protection Policy and Procedures

Policies and procedures shall be developed, documented, disseminated, and reviewed/updated annually or if there is a significant change to facilitate implementing physical and environmental protection controls.

21.2 PE-2 Physical Access Authorization

Designated officials or designees within the contractor's organization shall develop, review, keep current, and approve the access list and authorization credentials, i.e. identification (ID) badges. ID cards issued to employees and the card key inventory must be reconciled at least annually. The access list to the information and areas handling and processing SBU information shall also be updated at least annually.

If a contractor company is of limited size and the company manager/owner can sufficiently visually identify all individuals working at the facility, worn badges will not be required. Any contractor company with over 25 employees would be required to have a badging system in place. In the event that an inspection is taking place, an employee may be requested to provide verification of identity to an authorized government agent. Additionally, the contractor shall have a procedure to issue, manage, and track ID cards for visitors.

Otherwise, the contractor company shall issue and manage badges to enable employees assigned to IRS work to be readily identified. The authorization of employees must be reconciled periodically. Any time an employee departs the organization, the access/list and identification badge must be updated so that access is modified or deleted within 24 hours, as required. Employees must be made aware that ID media (identification cards) must be used for authorized access. Media should be safeguarded to prevent unauthorized use. All lost/stolen ID cards must be reported to management, as soon as loss is identified.

21.3 PE-3 Physical Access Control

When designating an area as limited access, it is important to ensure that management controls of the area are in place. This shall apply to all areas where access may be made into a secured perimeter. Examples of areas that may require additional protection may include stairwell doors and loading dock areas.

The contractor shall control all access points to the facility. This shall not apply to areas officially designated as publicly accessible. The contractor shall ensure that access is authorized and verified before granting access to areas where IRS information is processed or stored.

Prior to authorizing access to facilities and/or areas where IRS information is processed, visitors shall be authenticated. This does not apply to areas designated as publicly accessible.

The entry control monitor shall verify the identity of visitors by comparing the name and signature entered in the register with the name and signature of some type of photo identification card, such as a driver's license. When leaving the area, the entry control monitor or escort shall enter the visitor's time of departure. Each register shall be closed out at the end of each month and reviewed by the area supervisor/manager.

Whenever visitors enter the area, the contractor shall capture the following information: their name, signature, assigned work area, escort, purpose of entry, and time and date of entry.

See Appendix D for additional guidance on physical access controls.

21.4 PE-4 Access Control for Transmission Medium

The contractor shall physically control and monitor access to transmission lines and closets within the contractor facilities using physical safeguards. Security safeguards to control physical access to information system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

21.4.1 Transporting IRS Material

Any time SBU information is transported from one (1) location to another, care shall be taken to provide safeguards. In the event the material is hand-carried by an individual in connection with a trip or in the course of daily activities, it shall be kept with that individual and protected from unauthorized disclosures. For example, when not in use, and definitely when the individual is out of their hotel room, the material is to be out of view, preferably in a locked briefcase or suitcase.

All shipments of SBU information (including electronic, optical or other removable media and microfilm) shall be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All SBU information transported through the mail or courier/messenger service shall be double-sealed; that is one (1) envelope within another envelope. In addition, the address shall be contained on both the outer and inner envelope. The inner envelope shall be marked SBU with some indication that only the designated official or delegate is authorized to open it. Using sealed boxes serves the same purpose as double sealing and prevents anyone from viewing the contents thereof. All removable media must be encrypted, in accordance with the current encryption standard FIPS 140-2.

As practical, computers and IT media as well as sensitive information shall be secured when in hotel rooms, when hotel room is unattended.
When transporting IRS SBU material, the contractor shall ensure that material shall be safeguarded at all times during transport.

Methods to secure material shall include, but not be limited to, sealed envelopes; locked/electronically secured media transport containers, etc.

Any information stored in an automobile shall be stored in the trunk. If impractical, the information should be covered from view.

Ensure the courier vehicle is locked and secured when in possession of IRS data and/or remittances.

Ensure the vehicles used by the couriers are:

- Maintained in good condition, appearance and working order.
- Enclosed to ensure the packages and/or containers carried by the vehicle are secure.
- The vehicle must be secured. Vehicle doors must be secured (doors closed and locked) during transportation of the IRS packages or containers. All windows must be up in the vehicle during the transportation of data and remittances.
- The areas of the vehicles in which the packages and/or containers are placed, must be clear and debris-free. Other items are not to be commingled with the packages and/or containers.

21.5 PE-5 Access Control for Output Devices

The contractor shall control physical access to the information system devices that display IRS information or where IRS information is handled or processed to prevent unauthorized individuals from observing the display output.

21.6 PE-6 Monitoring Physical Access

The contractor or designee shall monitor physical access to SBU information and the information systems where IRS information is stored to detect and respond to physical security incidents. Physical access logs shall be reviewed annually or upon occurrence of or potential indication of an event.

Physical security Intrusion Detection Systems (IDS) are designed to detect attempted breaches of perimeter areas. IDS can be used in conjunction with other measures to provide forced entry protection for after-hours security. Additionally, alarms for individual and document safety (fire) and other physical hazards (water pipe breaks) are recommended. Alarms shall annunciate at an on-site protection console, a central station, or local police station. Physical security IDS include, but are not limited to door and window contacts, magnetic switches and motion sensors designed to set off an alarm at a given location when the sensor is disturbed.

Control Enhancement:

- The contractor shall monitor real-time physical intrusion alarms and surveillance equipment.

21.7 PE-8 Visitor Access Records

The contractor shall maintain visitor access records to the facility where the information system resides. Visitor access records are not required for publicly accessible areas.

The visitor access log shall contain the following information:

- Name and organization of the visitor,
- Signature of the visitor,
- Form of identification,
- Date of access,
- Time of entry and departure,
- Purpose of visit, and
- Name and organization of person visited.

Designated officials or designees within the contractor organization shall review the visitor access records, at least annually.

The contractor shall maintain visitor access records to the facility where the information system resides. Visitor access records are not required for publicly accessible areas.

The restricted area registers must be retained for at least a year.

21.8 PE-9 Power Equipment and Cabling

The contractor shall protect power equipment and power cabling for the information system from damage and destruction.

21.9 PE-10 Emergency Shutoff

Access to the shutoff switches or devices shall be unobstructed and located in such a manner so personnel have safe and easy access to them. The shutoff switches or devices are to be protected from unauthorized or inadvertent activation. The capability to shut off power to the information system or individual system components in emergency situations shall be provided.

21.10 PE-11 Emergency Power

The contractor shall provide a short term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a loss of primary power.

21.11 PE-12 Emergency Lighting

The contractor shall employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage that covers emergency exits and evacuation routes within the facility.

21.12 PE-13 Fire Protection

The contractor shall maintain fire suppression, detection, and notification (alarms) devices for the information and/or information systems.

Class A and Class C fire extinguishers shall be prominently located within any office complex containing IT assets so that an extinguisher is available within 50 feet of travel. Devices shall be supported by an independent power source and appropriate for the size of the facility being protected/safeguarded.

Control Enhancements:

- The contractor shall employ an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.
- When the facility is used to store large volumes of SBU information in warehouse and/or storage facilities, the contractor shall ensure that sprinkler systems and/or water suppression equipment shall be in place to minimize damage to critical historical files.

21.13 PE-14 Temperature and Humidity Controls

The contractor shall maintain and monitor temperature and humidity levels within the facility where the information system resides. The monitoring of the temperature and humidity levels is to be continuously monitored.

21.14 PE-15 Water Damage Protection

The contractor shall protect the information systems from damage resulting from water leakage by ensuring that master shutoff valves are accessible, working properly and known to key personnel.

21.15 PE-16 Delivery and Removal

For all IT information systems that house SBU information, the contractor shall authorize and control information system-related items entering and exiting the facility, and maintain appropriate records of those items.

The authorization process shall define individuals who are authorized to remove IT related equipment and/or other records.

If mailrooms are used, controls shall be put in place to ensure mail is also controlled, once received.

21.16 PE-17 Alternate Work Site

In all instances, the contractor shall employ appropriate management, operational, and technical information system security controls at alternate work sites. The effectiveness of security controls shall be assessed at the alternate work site.

The contractor shall develop procedures required to safeguard information for work performed at alternate work sites. The IRS reserves the right to inspect alternate work sites of a contractor. In addition, the contractor shall also provide a means for employees to communicate with information security personnel in case of security incidents or problems.

22 Planning (PL)

A contractor is responsible for planning for the security of information and IT assets throughout the life of the contract. This allows the contractor to ensure all security controls have been evaluated and implemented, as necessary and provides this assurance to the IRS.

22.1 PL-1 Security Planning Policy and Procedures

Policies and procedures shall be developed, disseminated, and reviewed/updated annually or if there is a significant change to formal documented requirements to complete a security plan and to address how these plans shall be updated and maintained.

22.2 PL-2 System Security Plan

The contractor shall develop and maintain a security plan to identify key information about the contractor site and about the security controls that shall be used to ensure that IRS information is adequately safeguarded.

The contractor shall plan and coordinate security related activities, such as security assessments, audits, information system hardware and software maintenance, and contingency plan testing, etc., affecting the information system. For example, the contractor would coordinate a vulnerability assessment and penetration testing.

Security plans are designed to document the security controls surrounding an information system environment. The contractor security plan shall ensure that security controls surrounding the contractor site environment have been adequately documented and safeguard mechanisms are in place.

Each year, the contractor shall provide a security plan as part of the State of Security package to the IRS that shall include the following:

- Administrative Information Cover: Include information such as contractor name, location of facilities handling IRS SBU information or information systems, points of contract (e.g., Project Manager, Information System Administrator, Security Officer) (to include telephone number and email address), contract/order number, period(s) of performance, dollar value (by performance periods), business size and socioeconomic characteristics, etc.
- Employee Roster: Identify all contractor employees working on the contract, and annotate those that have access to or handle SBU information, or have access to or operate or work with information systems containing SBU information. In addition, verify which contractor employees have or have not completed the current annual requirements for the Security Awareness Training. Employer roster should also include Minimum Background Investigation (MBI) status.
- Subcontractor Support: Names and addresses of contractor and all subcontractors performing IRS work.
- Infrastructure Diagram: Provide a diagram providing a general picture of the IT assets being used.

- Inventory of IT Assets: Provide an inventory of the type of equipment being used, including IT equipment/component, number of components, associated serial numbers, and location.
- Explicitly defines the authorization boundary for the system.
- Provides the security categorization of the information system including supporting rationale.
- Reviewed annually.
- Protect the security plan from unauthorized disclosure and modification.

Additional reference information for completing a security plan can be obtained from the NIST Web site: NIST SP 800-18 Revision 1, Developing Security Plans for Federal Information Systems.

Control Enhancements:

- The contractor shall plan and coordinate security-related activities affecting the information system with appropriate contractor groups/organizations before conducting such activities in order to reduce the impact on other contractor entities.

22.3 PL-4 Rules of Behavior

The contractor shall develop a set of expected rules of behavior when processing or handling IRS information. For all contractor employees who have access to IRS information, the contractor employee shall provide a signed acknowledgement indicating their understanding of these roles and responsibilities. The rules of behavior only need to be re-signed by the users if/when they are updated. Acknowledgement shall be made annually by personnel who have access to contractor managed IT assets. The Rules of Behavior must be reviewed annually and updated as necessary.

Control Enhancements:

- The contractor shall include in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting contractor information on public websites.

22.4 PL-8 Information Security Architecture

The contractor shall develop and maintain an Information Security Architecture document that:

- describes the overall security architecture of the organization;
- describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
- describes how the information security architecture is integrated into and supports the enterprise architecture; and
- describes any information security assumptions about, and dependencies on, external services.

The document shall be reviewed annually and updated as necessary. The architecture document should be scaled to the size of the IT environment.

The contractor shall ensure that architecture concepts are also included and integrated into the appropriate security documents including the Security Plan, IT Contingency Plan, procurement planning and other similar documents. Planned information security architecture changes are to be reflected in the security Concept of Operations (CONOPS).

23 Program Management (PM)

N/A - Does not apply to contractors. The IRS is primarily responsible for Program Management controls.

24 Personnel Security (PS)

All contractor and subcontractor employees performing or proposed to perform under the contract are identified to the IRS at time of award (or assignment) in order to initiate appropriate background investigations. Any contractor personnel that are not favorably adjudicated or otherwise pose a security risk are immediately removed from performance under contracts with the IRS, and suitable replacement personnel agreeable to the IRS are provided.

24.1 PS-1 Personnel Security Policy and Procedures

The contractor shall develop, document, and disseminate personnel security policies and procedures and review/update them annually or if there is a significant change. The policy shall define the need for all contractor personnel to obtain an approved IRS security screening (interim or final) before working on IRS contract work.

24.2 PS-2 Position Risk Designation

At the start of any contract, the IRS Personnel Security office shall define the position risk categorization, and identify the type of background check required for that contract. The IRS will review and updated position risk categorizations annually. The COR shall coordinate within the IRS to ensure that all positions have been appropriately risk categorized, as required.

IRS approved staff-like access (interim or final background investigation) is also required for any personnel who configure computers, IT assets, or computer systems for the contractor, manage servers in an administrative capacity, have access to maintain and manage routers, or in any other way have the ability to access IRS information and facilities housing IRS information. This would include contractors who design, operate, repair, or maintain information systems, and/or require access to SBU information.

24.3 PS-3 Personnel Screening

Personnel screening shall take place for all contractor personnel who work on IRS contracts. This includes employees who perform data entry, develop or write programs, perform assessments for tax purposes, perform security or telecommunications

administration to the information system, or have staff-like access to data or information systems. This also includes subcontractors who support the primary contractor efforts.

Contractor employees who are assigned to IRS contract work shall meet the following standards:

Eligibility

1. A contractor employee shall meet minimum citizenship requirements:
    a. A contractor employee with high risk access is required to be a United States citizen;
    b. A contractor employee with moderate risk access is required to be, at a minimum, a lawful permanent resident with three (3) years of US residency;
    c. A contractor employee with low risk access is required to be, at a minimum, a lawful permanent resident;
2. The contractor employee shall be tax compliant and remain tax compliant for the time they are on the contract;
3. If male and born after 1959, the contractor employee shall be registered with Selective Service in accordance with applicable laws and regulations.

Suitability - A contractor employee shall be fingerprinted and shall have favorable results from a check of the FBI fingerprint database and the local police fingerprint database. For high risk access, the contractor employee shall also have a successfully adjudicated investigation. Contractors who are deemed to be eligible and suitable shall be granted staff-like access to IRS information systems, facilities, and SBU information and shall follow IRS policies regarding the use and protection of those resources.

For contractor-managed resources housing IRS information outside the IRS firewall, staff-like access shall only be granted to those contractor employees who have been deemed by IRS to be eligible and suitable. The contractor is responsible for ensuring that only authorized personnel have access to these resources, that these authorized personnel understand how to protect the resources, that access requirements are reviewed and adjustments are made as authorized personnel change job duties, and that access is removed for any authorized personnel who are no longer assigned to IRS contract work. The contractor shall advise the IRS of any changes made to authorized personnel access privileges.

The contractor shall screen individuals prior to authorizing access to the information system. Only individuals who have passed an IRS background investigation shall be allowed access to IRS sensitive information.

24.4 PS-4 Personnel Termination

Within 3 working days of termination of an individual's employment the contractor shall terminate information system access, retrieve all security-related contractor information system-related property; and retain access to contractor information and information systems formerly controlled by terminated individual. Upon termination of any user who

has elevated privileges, access must be immediately revoked. The contractor shall terminate/revoke any authenticators/credentials associated with the individual. Within 5 working days the IRS COR and CSM shall be notified of termination of employees assigned to the contract.

24.5 PS-5 Personnel Transfer

The contractor shall review logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the contractor organization and when warranted retrieve all security-related contractor information IT asset-related property; and retain access to contractor information and information systems formerly controlled by a transferred individual. The contractor shall modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer and notify the IRS COR and CSM when an employee on the contract is transferred.

24.6 PS-6 Access Agreements

The contractor shall ensure that individuals requiring access to SBU information and information systems containing SBU information sign appropriate access agreements prior to being granted access and shall review/update the access agreements to ensure that they are accurate and current annually.

24.7 PS-7 Third-Party Personnel Security

The contractor shall establish personnel security requirements including security roles and responsibilities for third-party providers. Third party personnel security requirements shall be documented and monitored for compliance. The contractor shall monitor third party provider compliance and requires third-party providers to notify the primary contractor, who will notify IRS COR of any personnel transfers or terminations of third-party personnel who possess contract credentials and/or badges, or who have information system privileges. All contractors and subcontractors providing IT support shall meet the personnel security requirements of the primary contractor, as they have staff-like access to the data.

24.8 PS-8 Personnel Sanctions

A formal sanctions process for personnel failing to comply with established information security policies and procedures shall exist and be followed. The contractor shall notify the COR when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

25 Risk Assessment (RA)

Risk assessment controls ensure that risk can be assessed within the contractor, and that appropriate mitigation controls can be implemented.

25.1 RA-1 Risk Assessment Policy and Procedures

For any contractor using information systems, a risk assessment policy and procedure shall be developed, documented, disseminated and reviewed/updated annually or if there is a significant change to facilitate implementing risk assessment controls. Such risk assessment controls include risk assessments and risk assessment updates.

25.2 RA-2 Security Categorization

In general, contracts containing SBU information for tax administration purposes shall be assigned a security categorization of Moderate. This security categorization has been established by the IRS in accordance with federal laws, Executive Orders, directives, policies, regulations, standards and guidance, specifically (FIPS) 199.

25.3 RA-3 Risk Assessment

For all information systems environments, a risk assessment shall be conducted by the contractor to assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency regarding the use of SBU information. The contractor shall review the risk assessment results annually and update the risk assessment every three (3) years or whenever there is a significant change to the information system or environment in which it operates.

25.4 RA-5 Vulnerability Scanning

Vulnerability scanning is a test that inspects workstations, servers, network or mobile computing devices for weaknesses or flaws. The test relies on vulnerability scanning software that shall be configured to inspect devices for missing updates, patches and common configuration problems. The software shall be configured to receive updates and have the capability to perform authenticated scanning. All workstations, servers, network or mobile computing devices shall undergo monthly vulnerability scanning.

Any time a contractor is using IT assets, such as a workstation, laptop, server, etc., the contractor shall ensure there are scanning tools in place to ensure that no vulnerabilities are introduced into the environment. At a minimum, virus detection is required to ensure malicious software is not introduced into the environment.

Whenever a contractor is using networks, including LANs or WANs, the contractor shall conduct more sophisticated network scanning methods such as Network Intrusion Detections or Host Intrusion Detection to identify and correct potential network weaknesses.

The vulnerability scanning tools used shall include the capability to readily update the list of information system vulnerabilities scanned. These reviews shall be done monthly or when significant new vulnerabilities affecting the information system are identified and reported.

When providing programming services or hosting applications or services, enhanced vulnerability scanning software shall also be used. Enhanced vulnerability scanning software is capable of inspecting source code for common security flaws and performing dynamic build testing that inspects the application for security flaws at run time. Prior to deployment or delivery, static source code analysis and dynamic build testing shall be performed. Enhanced vulnerability scanning shall be performed whenever changes are made and dynamic build testing shall be performed on a

monthly basis.

The output and results of monthly vulnerability scanning, static source code analysis and dynamic build testing shall be retained for the duration of the contract and provided to the COR or auditors when requested.

Control Enhancements:

- The contractor shall employ vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.
- The contractor shall update the information system vulnerabilities scanned at least annually.
- The information system implements privileged access authorization to all information system components (As applicable (e.g., Operating System, Database, Web Application, etc.)

26 System and Services Acquisition (SA)

Information system and services acquisition controls ensure that security is planned into the environment whenever IT assets are being evaluated and/or procured for use.

26.1 SA-1 System and Services Acquisition Policy and Procedures

The contractor shall develop, document, disseminate, and review/update policies and procedures annually or if there is a significant change to ensure adequate information system and services acquisition policies are developed and implemented.

26.2 SA-2 Allocation of Resources

The contractor shall ensure that security capabilities are procured to be used in conjunction with IT capabilities for IT assets, such as laptops, workstations, or servers.

If the contractor is managing a network or information system, the contractor shall ensure the need for security tools is assessed, as procurements are made for information technology components. The contractor shall determine, document, and allocate as part of its capital planning and investment control process the resources required to adequately protect the IT information system and/or application programs.

26.3 SA-3 System Development Life Cycle

Whenever information systems contain SBU information, the contractor shall manage the information system using an information system development life cycle methodology that includes information security considerations.

For contractors having a limited number of items of tax information or a limited access to SBU information, the contractor shall implement controls to ensure that information and information systems are protected from the time they are received until the time these are returned to the IRS or the contract has ended. The security roles and responsibilities are assigned to specific individuals responsible for information security.

26.4 SA-4 Acquisition Process

When information systems contain SBU information, the contractor shall include security requirements and/or security specifications on all acquisition contracts, used by the contractor.

Control Enhancements:

- The contractor shall require the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed. The CO/COR shall define the level of detail required in the required information.
- The contractor shall require the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics.
- The contractor shall require the developer of the information system, system component, or information system service to identify early in the system development life cycle the functions, ports, protocols, and services intended for contractor use.
- The contractor shall employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within contractor IT assets.

26.5 SA-5 Information System Documentation

The contractor shall ensure that adequate documentation for the IT information system and/or application programs and the constituent components are available, protected when required, and distributed to authorized personnel.

26.6 SA-8 Security Engineering Principles

When information systems contain SBU information, the contractor shall design and implement the information system using security engineering principles.

Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions.

26.7 SA-9 External Information System Services

The contractor shall require providers of external information system services to comply with information security requirements, and employ appropriate security controls in accordance with applicable federal law. Government oversight and user roles and responsibilities with regard to external information system services shall be defined and documented. Security control compliance by external service providers shall be monitored.

Control Enhancements:

- The organization requires providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.

26.8 SA-10 Developer Configuration Management

The contractor shall require that information system developers perform configuration management during information system design, development, implementation and operation. Changes to the information system shall be controlled, approved and documented. Security flaws and resolution shall be tracked. This applies to contractors who provide design and development support to the IRS.

The information system developers shall create a security test and evaluation plan, implement the plan, and document the results.

26.9 SA-11 Developer Security Testing and Evaluation

Contractors who perform development work for the IRS shall ensure that testing is conducted for the developer environment. At a minimum, the contractor shall:

- Create and implement a security test and evaluation plan.
- Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process.
- Document the results of the security testing/evaluation and flaw remediation processes.
- Ensure the results of the tests are communicated to the IRS organization.
- Perform system testing and evaluation that include one or more of the following:
    - Security-related functional properties
    - Security-related externally visible interfaces
    - High-level design
    - Low-level design
    - Implementation representation (source code/hardware schematics)
    - Correct flaws identified during security testing/evaluation.

27 System and Communications Protection (SC)

A secure information system communication ensures that information is protected from unauthorized disclosure or tampering during transit, and ensures that the network

communication paths, where IT assets are being used to transmit IRS SBU information, are protected.

27.1 SC-1 System and Communications Protection Policy and Procedures

The contractor shall develop, document, disseminate, and review/update policies and procedures annually or if there is a significant change to ensure adequate information system and communications protection policies are developed and implemented.

27.2 SC-2 Application Partitioning

For all contractors who manage IT development and production application environments, the information system shall physically and/or logically separate user functionality (including user interface services) from information system management functionality, and ensure that the separation functions are implemented and enforced.

27.3 SC-4 Information in Shared Resources

The information system prevents unauthorized and unintended information transfer via shared information systems resources.

27.4 SC-5 Denial of Service Protection

Contractors shall ensure that all IT assets and information systems are protected against or limit the effects of denial of service attacks, using boundary devices such as firewalls and routers, etc.

27.5 SC-7 Boundary Protection

Any contractor who manages information system environments shall ensure that all internal and external information system boundaries are controlled using boundary protection mechanisms, e.g. routers and switches. In addition, the contractor shall ensure management personnel monitor, control, and report all accesses made through routers or switches. The communications at the external boundary are to be monitored, in addition to being controlled.

Control Enhancements:

- The contractor shall limit the number of external network connections to the information system.
- The contractor shall:
  - (a) Implement a managed interface for each external telecommunication service.
  - (b) Establish a traffic flow policy for each managed interface.
  - (c) Employ security controls as needed to protect the confidentiality and integrity of the information being transmitted across each interface.
  - (d) Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need.
  - (e) Review exceptions to the traffic flow policy annually.
  - (f) Remove traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

- The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).
- The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

27.6 SC-8 Transmission Confidentiality and Integrity

The information system protects the confidentiality and integrity of transmitted information. Encryption shall be compliant with FIPS 140-2 or later protection requirements.

27.7 SC-10 Network Disconnect

The information system shall disconnect all network connections upon session completion or after 30 minutes of inactivity. This requirement does not apply to VPN sessions connecting to the IRS network.

27.8 SC-12 Cryptographic Key Establishment and Management

The contractor shall establish and manage cryptographic keys for required cryptography employed within the information system. When public key certificates are used, the contractor shall manage key policies and/or certificates. The IRS shall notify a contractor if they are using public key concepts and certificates.

27.9 SC-13 Cryptography Protection

When cryptography (encryption) is employed within the information system, the information system shall perform all cryptographic operations using FIPS 140-2 or later 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/validation.html.

27.10 SC-15 Collaborative Computing Devices

Collaborative devices shall have their remote activation capability removed/disabled. This is to prevent the device from being activated when a user is not physically present. The collaborative device shall also provide an indicator to the users present that the device is active. Collaborative computing devices include, but are not limited to video and/or audio conferencing capabilities.

27.11 SC-17 Public Key Infrastructure Certificates

For all contractors who manage information systems, the information system shall document processes with supporting procedures for digital certificate generation, installation, and distribution. Subscriber key pairs are generated and stored using FIPS 140-2 or later Security Level 2 or higher cryptographic modules. The same public/private key pair is not to be used for both encryption and digital signature. Private keys are protected using, at a minimum, a strong password. A certificate is revoked if the associated private key is compromised; management requests revocation; or the certificate is no longer needed.

27.12 SC-18 Mobile Code

The contractor shall define acceptable and unacceptable mobile code and mobile code technologies. Usage restrictions and implementation guidance shall be established for acceptable mobile code and mobile code technologies. The contractor shall authorize, monitor, and control the use of mobile code within the information system.

Mobile code is software that is executed from a host machine to run scripts on a client machine, including animation scripts, movies, etc. Mobile code is a powerful computing tool that can introduce risks to the user's information system. Whenever a contractor is developing or deploying the mobile code technology, this shall be identified in the contractor's security plan to the IRS. Contractors, who use mobile code, shall be subject to a source code review by IRS personnel to ensure that there is no potential risk in introducing malicious code into the contractor/user's environment.

27.13 SC-19 Voice over Internet Protocol (VoIP)

The contractor shall establish, document, and control usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause unintentional disclosure of SBU information. Appropriate contractor officials shall authorize the use of VoIP. This shall be identified in the security plan to the IRS.

27.14 SC-20 Secure Name/Address Resolution Services (Authoritative Source)

When information system networks are in use, domain location naming and location services shall be implemented to ensure the integrity and authorization of all devices contained within that domain environment.

The information system, when operating as part of a distributed system shall employ mechanisms to be able to establish and validate trust among all servers being used within the environment.

This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A Domain Name Server (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. The DNS security controls are consistent with, and referenced from OMB Memorandum 08-23:
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf

27.15 SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

The information system shall use data authentication and integrity verification procedures for all communications among servers within the corporate infrastructure, used for IRS business functions.

27.16 SC-22 Architecture and Provisioning for Name/Address Resolution Service

Fault-tolerance is a capability that allows an information system or application to continue operation when components of the original information system or application fail. Whenever a contractor has name/address resolution service implemented, this shall be fault-tolerant and implement internal/external role separation. The fault tolerance shall ensure that if a name cannot be reconciled, the information system or application shall continue to operate normally, but return the error regarding the name resolution.

Related to role separation, information systems with an internal role (operating inside the contractor) shall perform name resolution only on internal servers. Likewise, those information systems with external roles (outside of the contractor) shall perform name resolution for those servers outside of the contractor site.

27.17 SC-23 Session Authenticity

The information system shall provide mechanisms to protect the authenticity of communications sessions that shall validate the source and destination of communication sessions. This applies to contractors, who are developing or providing web-based applications. This establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.

27.18 SC-28 Protection of Information at Rest

All portable media shall be encrypted, including laptops, backup data, etc.

27.19 SC-39 Process Isolation

The information system maintains a separate execution domain for each executing process. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one (1) process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multi-state processor technologies.

NOTE: This control is only applicable for CSOFT.

28 System and Information Integrity (SI)

This section applies to contractors who are developing application programs, web-based interface applications, surveys that can be completed by a user population, and other instances where input data could be manipulated, causing inaccurate information to be generated. For each control, there shall be a note on the applicability to a contractor site.

28.1 SI-1 System and Information Integrity Policy and Procedures

Information system and information integrity policy and procedures shall be developed, disseminated and reviewed/updated annually or if there is a significant change to facilitate implementing information system and information integrity security controls.

28.2 SI-2 Flaw Remediation

Contractors shall identify, report, and correct information system flaws. The contractor shall promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes). Software and firmware updates related to flaw remediation shall be tested for effectiveness and potential side effects before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling shall be addressed expeditiously. The contractor shall incorporate flaw remediation into their configuration management process. This allows for the required/anticipated remediation actions to be tracked and verified.

Control Enhancements:

- The contractor shall employ automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation.

28.3 SI-3 Malicious Code Protection

The information system and/or application programs shall implement malicious code protection that includes a capability for automatic updates. Examples of malicious code include viruses, worms, spyware, Trojan horses, etc. The contractor shall weekly scan the IT assets for malicious code, and identify actions that shall occur in the event malicious code is detected. Possible actions include quarantine of malicious code, eradication, etc. Virus protection software shall be installed on all workstations, servers, or mobile computing devices. The virus detection software shall be configured to perform automated updates on a daily basis, and perform automated scanning of all files, incoming and outgoing emails or other network communications. The contractor shall address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Removable media, for example, USB devices, diskettes, or compact disks, shall be scanned whenever they are connected to a computing device.

Malicious code protection mechanisms shall be employed at information system entry and exit points to detect and eradicate malicious code. Procedures shall be defined to institute malicious code detection as a centrally managed process. In addition, the contractor shall define how updates are reviewed and applied. Users of the information system shall not be able to bypass malicious code protection controls implemented by management. All contractors, including those in small company environments, shall ensure they have procured and installed software to enable malicious code to be detected and acted upon.

Control Enhancements:

- The contractor shall centrally manage malicious code protection mechanisms.

- The information system automatically updates malicious code protection mechanisms (including signature definitions).

28.4 SI-4 Information System Monitoring

The contractor shall employ tools and techniques to monitor events on the information system to detect attacks, vulnerabilities, and detect, deter, and report on unauthorized use of the information system. The information system is to be monitored for unauthorized local, network, and remote connections. Whenever there is an elevated security level, the monitoring efforts shall be increased as necessary to enable deterrence, detection, and reporting to take place so that corrective actions shall be made to the networked environment. Information obtained from intrusion-monitoring tools shall be protected from unauthorized access, modification, and deletion.

Contractors with small IT environments, (e.g., using personal information systems) shall meet the intent of this control by implementing antivirus and firewall protection tools to monitor and protect them from cyber-attacks:

- Automated tools for near real time analysis.
- Monitors inbound and outbound communications for unusual activity.
- Provides near real time alert regarding potential compromise.
- Prevents users from bypassing capabilities.

All contractors, including those in small company environments, shall ensure they have procured and installed software to enable vulnerability detection to take place.

Control Enhancements:

- The contractor shall employ automated tools to support near real-time analysis of events.
- The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.
- The information system provides near real-time alerts when the following indications of compromise or potential compromise occur.

28.5 SI-5 Security Alerts, Advisories, and Directives

For all information systems, the contractor shall ensure that they receive information system security alerts/advisories on a regular basis, generates internal security alerts, advisories, and directives as deemed necessary, issue alerts/advisories to appropriate personnel, and take appropriate actions as necessary. The contractor shall define appropriate personnel within the organization who shall receive the alerts/advisories, and who has responsibilities to act on these. All contractors, including those in small company environments, shall ensure they have procured and installed software to enable software advisories to be received and acted upon.

28.6 SI-7 Software Firmware, and Information Integrity

The contractor shall employ integrity verification tools to information systems, which shall detect and protect against unauthorized changes to software, firmware, and information. If an unauthorized change occurs, the contractor shall use configuration

management practices to enable the information system or application to be restored to the correct operational state. Procedures shall be established to enable data to be corrected. Auditing concepts shall be applied to enable identification of the events that caused the unauthorized change and take actions as necessary. All contractors, including those in small company environments, shall ensure they have procured and installed software to enable the information system to prevent unauthorized software to be installed.

When information systems contain SBU information, the contractor shall comply with software copyright usage restrictions. The contractor shall enforce explicit rules governing the downloading and installation of software by users.

Control Enhancements:

- The information system performs an integrity check of software, firmware, and information at:
  a. Startup;
  b. The identification of a new threat to which the information system is susceptible;
  c. The installation of new hardware, software, or firmware; and
- The contractor shall reassess the integrity of software and information by performing annual integrity scans of the information system.

28.7 SI-8 Spam Protection

Contractors shall employ and maintain up-to-date spam protection mechanisms at information system entry, exit points, and at the workstations. Server or mobile computing devices shall be on the network to detect and take action on unsolicited messages transported by electronic mail, mail attachments, web access or other common means. All contractors, including those in small company environments, shall ensure they have procured and installed software to enable spam protection within the email environment, if this is contained on the same asset used to conduct IRS work.

Control Enhancements:

- The contractor shall centrally manage spam protection mechanisms.
- The information system automatically updates spam protection mechanisms.

28.8 SI-10 Information Input Validation

For any applications developed by contractors, developers shall ensure that consistency checks for input validation are defined and used to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and injection attacks.

28.9 SI-11 Error Handling

The information system shall identify security relevant error conditions and handle error conditions in an expeditious manner. Procedures shall be developed to enable errors to be identified and corrected. In addition, errors shall not expose information to others that could allow the information system or application to be compromised. An example of an error message a user may receive is when they type either their user ID or

password incorrectly. The error message notifies the user they cannot be logged in, but it does not tell them if they provided an invalid user ID or password.

28.10 SI-12 Information Output Handling and Retention

Contractors shall handle and retain data within the information system, according to record retention standards. The IRS shall identify the record retention standards to the contractor. In addition, once the contract expires, all data shall be returned to the IRS, unless specifically identified otherwise in the contract. No records shall be maintained, in paper or electronically, unless approved by the IRS COR.

28.11 SI-16 Memory Protection

The contractor shall implement protection on any data asset used to process IRS information to protect its memory from unauthorized code execution. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

29 Privacy Controls

29.1 AR-3 Privacy Requirements for Contractors and Service Providers

The contractor shall ensure that IRS data is used only as specified in the IRS contract, and for no other purpose to protect the privacy of individuals whose data is processed in the information system. .

29.2 AR-5 Privacy Awareness and Training

Privacy awareness will be included within the IRS mandatory training. All contractor personnel who handle or process IRS PII shall be responsible for being aware of their privacy responsibilities.

29.3 DM-2 Data Retention and Disposal

Once disposal is complete, a copy of the disposal record and notification must be provided to the IRS CO/COR.

29.4 DM-3 Minimization of PII Used in Testing, Training, and Research

IRS provided PII shall not be used for testing, training, or research without the explicit permission of the IRS.

29.5 SE-1 Inventory of Personally Identifiable Information

The contractor is responsible for maintaining an inventory of all PII provided to the contractor, generated by the contractor, or used by the contractor sufficient to enable notification to taxpayers, if disclosed.

The inventory of PII must be updated semi-annually with a final inventory notification provided to the COR.

29.6 SE-2 Privacy Incident Response

The contractor shall develop and implement a Privacy Incident Response Plan that provides an organized and effective response to privacy incidents. All privacy-related incidents must be reported to the IRS as identified in Section 18.

30 Termination of Contract

At the end of the contract period, or if the contract is terminated within the contract period, the contractor shall coordinate with the IRS to ensure contractor and contractor employee access privileges to IRS information, IRS systems and facilities are revoked in a timely manner, as necessary.

Contractors shall confirm to IRS officials that information furnished under the contract has been properly returned, disposed, or destroyed.

Information and IT assets shall be returned to the IRS, destroyed and/or sanitized, as required or directed by the IRS. This includes assuring the IRS that all IT assets, including laptops, information systems, servers, routers, printers, faxes, switches, voice recordings, and all removable and fixed media have been sanitized of all IRS information prior to returning into production for other use.

Contractors required to return IRS information and property (as a part of the contract requirements) shall use a process that ensures that the confidentiality of the SBU information is protected at all times during transport.

A log shall be maintained to ensure that all media destroyed has identified the date of destruction, content of media, serial number, type of media (CD, DVD, Closed Caption Television (CCTV), etc.) destruction performed, personnel performing destruction, and witness.

All VoIP shall be sanitized prior to returning to production, when SBU information is stored on these devices.

All hard drives and removable media shall be inventoried, sanitized, and logged to demonstrate data destruction for all IT assets used to handle SBU data.

All hard copies shall be returned using double-wrapped envelopes and traceable mail.

30.1 Destruction or Return of SBU Information

When the contract is officially closed out, SBU information provided to the contractor or created by the contractor shall be returned to the IRS or destroyed as directed in writing by the IRS. This includes copies of reports, extra copies, photo impressions, information system printouts, carbon paper, notes, stenographic notes, and work papers.

Note: See Section 20 the Media Protection Control concerning Media Transport and Media Sanitation.

Contractors shall follow the approved IRS Records Office Record Control Schedule (RCS) that covers how records are retained or destroyed. The Business Owner shall have the records retention schedules available and built into the contract.

Destruction of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, cross-cut shredding, incineration, pulverizing, and melting. The shred size of the refuse shall produce particles that are no more than 1 x 5 millimeters in size. These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or incineration facility with the specific capabilities to perform these activities effectively, securely and safely.

Either an IRS employee or a contractor with an IRS approved background check shall be present during the incineration and/or destruction of SBU information. The employee shall be present and observe the destruction process.

31 Taxpayer Browsing Protection Act of 1997 and Unauthorized Access and Disclosures

The Taxpayer Browsing Protection Act of 1997 covers the willful unauthorized access or inspection of any taxpayer records, (the IRS calls this UNAX) including hard copies of returns and return information as well as returns maintained on an information system. Unauthorized access or inspection of taxpayer records (even if the information is not disclosed) is a misdemeanor.

This crime is punishable by fines and could also result in prison terms. The provisions and applicable criminal penalties under the Taxpayer Browsing Protection Act apply to all contractors, and contractor employees. Before any contractor employee can be given access to returns, they shall have received a properly adjudicated IRS background investigation, and certify that they have been provided UNAX training.

Once contractors have taken IRS required training, completion documentation shall be returned to the Contractor Security Management office, and to the Contracting Officer or designee. UNAX forms shall not be retained at the contractor site.

In addition, other briefings shall be provided to communicate security messages to employees. Security information shall be communicated using any of the following methods:

- Formal and informal training.
- Discussion at group and managerial meetings.
- Install security bulletin boards throughout the work areas.
- Place security articles in employee newsletters.
- Route pertinent articles that appear in the technical or popular press to members of the management staff.

- Display posters with short simple educational messages (e.g., instructions on reporting unauthorized access "UNAX" violations, address, and hotline number).
- Use warning banners during initial logon on information systems housing SBU information.
- Send e-mail and other electronic messages to inform users.

UNAX deals with the unauthorized access. In addition to UNAX, the contractor shall ensure that information is not disclosed to unauthorized personnel. In addition, UNAX addresses any inadvertent access (accidental) made by an employee or a contractor.

As part of the certification, and at least annually afterwards, contractor employees shall be advised of the provisions of IRC Sections 7213, 7213A and 7431 (See Exhibit 2– LEGAL REQUIREMENTS and Exhibit 3, Taxpayer Browsing Protection Act).

Note: Contractors shall make employees aware that disclosure restrictions and the penalties apply even after employment with the contractor has ended.

It shall be certified that contractor employees understand security policy and procedures requiring their awareness and compliance.

APPENDIX A: ACRONYMS

Acronym	Acronym Description
AAL	Authorized Access List
AC	Access Control
AR	Accountability, Audit, and Risk Management
AT	Awareness Training
AU	Audit and Accountability
ATM	Automated Teller Machine
AWSS	Agency Wide Shared Services
BOD	Business Operating Division
CA	Security Assessment & Authorization
CCTV	Closed Caption Television
CD	Compact Disc
CD-R	Compact Disc Recordable
CD-ROM	Compact Disc Read Only Memory
CD-RW	Compact Disc – Rewritable
CM	Configuration Management
CNET	Core (C) plus Network Information Technology Infrastructure (NET)
CO	Contracting Officer
CONOPS	Concept of Operations
COR	Contracting Officer's Representative
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off the Shelf Software
CP	Contingency Planning
CSA	Contractor Security Assessments
CSAT	Core (C) plus value greater than Simplified Acquisition Threshold (SAT)
CSOFT	Core (C) plus Software Application Development/Maintenance (SOFT)
CSPSA	Contractor Statements of Physical Security Assurance
CSSA	Contractor Statements of Security Assurance
CSM	Contractor Security Management
CSR	Contractor Security Representative
DM	Data Minimization and Retention
DNSS	Domain Name Server System
DVD	Digital Video Device

Acronym	Acronym Description
FAR	Federal Acquisition Regulation
FAX	Facsimile Machines
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act 2002. Amended 2014
FMSS	Facilities Management and Security Services
FTC	Federal Trade Commission
FTI	Federal Tax Information (see returns and return information)
FTP	File Transfer Protocol
GLB	Gramm-Leach Bliley
GSA	General Services Administration
IA	Identification & Authentication
IDS	Intrusion Detection Systems
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IR	Incident Response
IRC	Internal Revenue Code
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology (formally Modernization & Information Technology Services)
LAN	Local Area Network
LES	Law Enforcement Sensitive
MA	Maintenance
MAC	Media Access Control
MO	Magnetic-Optic
MP	Media Protection
MPS	Minimum Protection Standards
NAT	Network Address Translation
NET	Networked Information Technology
NIST	National Institute of Standards and Technology
OEP	Occupant Emergency Plan
OMB	Office of Management & Budget
PE	Physical & Environmental Protection
PED	Personal Electronic Device

Acronym	Acronym Description
PGLD	Privacy, Governmental Liaison and Disclosure
PKI	Public Key Infrastructure
PCLIA	Privacy and Civil Liberties Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PL	Planning
PM	Program Management
POA&M	Plan of Action and Milestone
PS	Personnel Security
RA	Risk Assessment
RCS	Record Control Schedule
ROM	Read Only Memory
RPO	Recovery Point Objective
RTO	Recover Time Objective
SA	System and Services Acquisition
SAMC	Situation Awareness Management Center
SAR	Security Assessment Report
SAT	Simplified Acquisition Threshold
SBU	Sensitive But Unclassified
SC	System and Communication Protection
SCAP	Security Content Automation Protocol
SE	Security
SI	System and Information Integrity
SOFT	Software Application Development or Maintenance
SoS	State of Security
SP	Special Publication
SQL	Structured Query Language
SSP	System Security Plan
TCP	Transmission Control Protocol
UL	Underwriters Laboratory
UNAX	Unauthorized Access
USB	Universal Serial Bus
USC	United States Code
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Networks

APPENDIX B: GLOSSARY

A

The IRS maintains a complete inventory of all its information systems based on the following classifications:

ACCOUNTABILITY: A process of holding users responsible for actions performed on an information system.

ADEQUATE SECURITY: Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of information.

ALTERNATE WORK SITE: Any working area that is attached to the Wide Area Network (WAN) either through a Public Switched Data Network (PSDN) or through the Internet.

ASSURANCE: A measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.

ASSURANCE TESTING: The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

AUDIT: An independent examination of security controls associated with a representative subset of contractor IT assets to determine the operating effectiveness of information system controls; ensure compliance with established policy and operational procedures; and recommend changes in controls, policy, or procedures where needed.

AUDIT TRAIL: A chronological record of information system activities sufficient to enable the reconstruction, reviewing and examination of security events related to an operation, procedure or event in a transaction, from its inception to final results.

AUTHENTICATION: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. See IDENTIFICATION.

AUTHORIZATION: Access privileges granted to a user, program or process.

AVAILABILITY: Timely, reliable access to information and information services for authorized users.

B

BANNER: Display of an information system outlining the parameters for information system or information use.

BASELINE SECURITY REQUIREMENTS: A description of the minimum security requirements necessary for an information system to enforce the security policy and maintain an acceptable risk level.

C

CLASSIFIED INFORMATION: National security information classified pursuant to Executive Order 12958.

COMPROMISE: The disclosure of sensitive information to persons not authorized to receive such information.

CONFIDENTIALITY: Preserving authorized restrictions on information access and disclosure.

CONFIGURATION MANAGEMENT: A structured process of managing and controlling changes to hardware, software, firmware, communications and documentation throughout the information system development life cycle.

CONTRACTING OFFICER'S REPRESENTATIVE: As defined in FAR Part 2, "'Contracting Officer's Representative (COR)' means an individual, including a Contracting Officer's Technical Representative (COTR), designated and authorized in writing by the contracting officer to perform specific technical or administrative functions."

CONTRACTOR SECURITY ASSESSMENTS: Contractor Security Assessments are on-site evaluations performed by the IRS to assess and validate the effectiveness of security controls established to protect IRS information and information systems.

CONTRACTOR SECURITY REPRESENTATIVE: The CSR is the contractor's primary point of contact 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.

COUNTERMEASURES: Actions, devices, procedures, mechanisms, techniques, or other measures that reduce the vulnerability of an information system.

CRYPTOGRAPHY: The process of rendering plain text information unreadable and restoring such unreadable information to a readable form.

D

DATA: A representation of facts, concepts, information, or instruction suitable for communication, processing, or interpretation by people or information systems.

DECRYPTION: The process of converting encrypted information into a readable form. This is also called deciphering.

DIGITAL SUBSCRIBER LINE: A public telecommunications technology delivering high bandwidth over conventional copper wire covering limited distances.

DISCRETIONARY ACCESS CONTROL: A method of restricting logical access to information system objects (e.g., files, directories, devices, permissions, rules) based on the identity and need to know of users, groups, or processes.

DOMAIN NAME SYSTEM: A hierarchical naming system that retains artifacts related to the lookup, including cryptographic keys, DNS resource records, etc.

E

ENCRYPTION: See CRYPTOGRAPHY.

ENCRYPTION ALGORITHM: A formula used to convert information into an unreadable format.

EXTERNAL INFORMATION SYSTEM: Information systems or components of information systems that are outside of the authorization boundary established by the contractor and for which the contractor typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness.

EXTERNAL NETWORK: Any network residing outside the security perimeter established by the telecommunications information system.

EXTRANET: A private data network using the public telephone network to establish a secure communications medium among authorized users (e.g., contractor, vendors, business partners). An Extranet extends a private network (often referred to as an Intranet) to external parties in cases where both parties may be benefit from exchanging information quickly and privately.

F

FILE PERMISSIONS: A method of implementing discretionary access control by establishing and enforcing rules to restrict logical access of information system resources to authorized users and processes.

FILE SERVER: A local area network information system dedicated to providing files and data storage to other network stations.

FIREWALL: Telecommunication device used to regulate logical access authorities between network information systems.

FIRMWARE: Microcode programming instructions permanently embedded into the Read Only Memory (ROM) control block of an information system. Firmware is a machine component of information system, similar to an information system circuit component.

G

GATEWAY: Interface providing compatibility between heterogeneous networks by converting transmission speeds, protocols, codes, or security rules. This is sometimes referred to as a protocol converter.

GENERAL SUPPORT SYSTEM: An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

H

HOST: An information system dedicated to providing services to many users. Examples of such information systems include mainframes, mini information systems or servers providing Dynamic Host Configuration Protocol (DHCP) services.

I

IDENTIFICATION: A mechanism used to request access to information system resources by providing a recognizable unique form of identification such as a login-id, user-id or token. Also, see AUTHENTICATION.

INFORMATION: See DATA.

INFORMATION SYSTEM: A collection of hardware, software, firmware, applications, information, communications and personnel organized to accomplish a specific function or set of functions under direct management control.

INFORMATION SYSTEM SECURITY: The protection of information systems and information against unauthorized access, use modification or disclosure – ensuring confidentiality, integrity and availability of information systems and information.

INTEGRITY: Protection of information systems and information from unauthorized modification; ensuring quality, accuracy, completeness, non-repudiation and authenticity of information.

INTRANET: A private network using TCP/IP, the Internet and world-wide-web technologies to share information quickly and privately between authorized user communities, including contractors, vendors and business partners.

K

KEY: Information used to establish and periodically change the operations performed in cryptographic devices for the purpose of encrypting and decrypting information.

L

LEAST PRIVILEGE: A security principle stating users or processes are assigned the most restrictive set of privileges necessary to perform routine job responsibilities.

M

MAJOR APPLICATION: An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and shall be treated as major. Adequate security for other applications shall be provided by security of the information systems in which they operate.

MALICIOUS CODE: Rogue information system programs designed to inflict a magnitude of harm by diminishing the confidentiality, integrity and availability of information systems and information.

N

NETWORK: A communications infrastructure and all components attached thereto whose primary objective is to transfer information among a collection of interconnected information systems. Examples of networks include local area networks, wide area networks, metropolitan area networks and wireless area networks.

NODE: A device or object connected to a network.

NON-REPUDIATION: The use of audit trails or secure messaging techniques to ensure the origin and validity of source and destination targets. That is, senders and recipients of information cannot deny their actions.

O

OBJECT REUSE: The reassignment of storage medium, containing residual information, to potentially unauthorized users or processes.

ORGANIZATION: A contracting company, agency, or any of its operational elements.

P

PACKET: A unit of information traversing a network.

PASSWORD: A private, protected, alphanumeric string used to authenticate users or processes to information system resources.

PENETRATION TESTING: A testing method where security evaluators attempt to circumvent the technical security features of the information system in efforts to identify security vulnerabilities.

PERSONALLY IDENTIFIABLE INFORMATION: The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

OMB 07-16: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

PLAN OF ACTION AND MILESTONE (POA&M): A management tool used to assist contractors in identifying, assessing, prioritizing, and monitoring the progress of corrective actions for security weaknesses found in programs and systems, as defined in OMB Memorandum 02-01.

POTENTIAL IMPACT: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect, a serious adverse effect, or a catastrophic adverse effect on contractor operations, contractor assets, or individuals.

PROTOCOL: A set of rules and standards governing the communication process between two (2) or more network entities.

PRIVACY AND CIVIL LIBERTIES IMPACT ASSESSMENT: A PCLIA is a process for examining the risks and ramifications of using information technology to collect, maintain and disseminate information in identifiable form about members of the public

and agency employees. The PCLIA also identifies and evaluates protections to mitigate the impact to privacy of collecting such information.

PUBLIC KEY INFRASTRUCTURE: PKI is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

R

RECOVERY POINT OBJECTIVE: The point in time to which data must be recovered after an outage.

RECOVERY TIME OBJECTIVE: The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business process.

REMNANTS: Residual information remaining on storage media after reallocation or reassignment of such storage media to different contractors, organizational elements, users or processes. See OBJECT REUSE.

RESIDUAL RISK: Portions of risk remaining after security controls or countermeasures are applied.

RETURNS AND RETURN INFORMATION: Includes all information protected by § 6103 of the Internal Revenue Code, 26 U.S.C. § 6103, commonly (and informally) referred to as Federal Tax Information (FTI).

RISK: The potential adverse impact to the operation of information systems affected by threat occurrences on contractor operations, assets and people.

RISK ASSESSMENT: The process of analyzing threats to and vulnerabilities of an information system to determining the potential magnitude of harm, and identify cost effective countermeasures to mitigate the impact of such threats and vulnerabilities.

RISK LEVEL: The security impact risk level is the low, moderate, or high impact level assigned to an information system in accordance with FIPS 199 and FIPS 200 based on the types of information processed, stored and/or transmitted by the information system.

RISK MANAGEMENT: The routine process of identifying, analyzing, isolating, controlling, and minimizing security risk to achieve and maintain an acceptable risk level. A risk assessment is an instrumental component of the risk management life cycle.

S

SAFEGUARDS: Protective measures prescribed to enforce the security requirements specified for an information system. This is synonymous with security controls and countermeasures.

SECURITY POLICY: The set of laws, rules, directives and practices governing how contractors protect information systems and information.

SECURITY REQUIREMENT: The description of a specification necessary to enforce the security policy. See BASELINE SECURITY REQUIREMENTS.

SENSITIVE BUT UNCLASSIFIED (SBU) INFORMATION: 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 (the Privacy Act of 1974), but which has not been specifically authorized under criteria established by an Executive Order or Congress to be kept secret in the interest or national defense for foreign policy.

SYSTEM: See INFORMATION SYSTEM.

SYSTEM SECURITY PLAN: An official document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. (NIST SP 800-18).

T

THREAT: An activity, event or circumstance with the potential for causing harm to information system resources.

U

USER: A person or process authorized to access an information system.

USER IDENTIFIER: A unique string of characters used by an information system to identify a user or process for authentication.

V

VIRUS: A self-replicating, malicious program that attaches itself to executable programs.

VULNERABILITY: A known deficiency in an information system that threat agents can exploit to gain unauthorized access to sensitive or classified information.

VULNERABILITY ASSESSMENT: Systematic examination of an information system to determine its' security posture, identify control deficiencies, propose countermeasures, and validate the operating effectiveness of such security countermeasures after implementation.

VULNERABILITY SCAN: A scan of the network environment, less invasive than a penetration test that can be used to identify information system vulnerabilities to a contractor's management.

APPENDIX C: SECURITY CONTROL LEVELS

All contractors are required to use the applicable Security Control Levels to ensure the protection of IRS SBU information and information systems, including contracting actions using Simplified Acquisition Procedures. If and when additional controls are required, these shall be defined in the contract. If and when a security control level other than what is described here or in Figure 1 or in applicable clauses to the contract as the norm or default level is to be used, then that security control level will be identified in the contract.

Figure 1 – Security Control Level High Water Mark (Hierarchy: Quadrant I – IV) of this appendix serves as a quick reference guide on the conditions and operators typical for each security control level within a hierarchy.

Figure 2 – Security Control Level Matrix (By Default Operators) of this appendix serves a quick reference guide for the contractor in selecting (applying for, and the CO determining) the security control level applicable to the immediate contracting action.

Table 8 – Table of Security Controls identifies the specific security controls applicable to each security control level.

Core Security Controls (**C**)
Core (C) + > Simplified Acquisition Threshold (SAT) = **CSAT**
Core (C) + Networked Information Technology Infrastructure (NET) = **CNET**
Core (C) + Software Application Development or Maintenance (SOFT) = **CSOFT**

Legend
The "high water" mark concept employs a hierarchy that goes from the least stringent security control level (core (C)) to the most stringent security control level (core + software (CSOFT)). It takes into account a number of risk-based factors and is responsive to individual users (e.g., individual, residential non-networked users) and business concerns of any size, with due deference to higher risk factors (operators) such as networked environments and software development).

Figure 1: Security Control Level High Water Mark (Hierarchy: Quadrant I – IV)

Core Security Controls = **C** All contracting actions for services that involve contractor access to SBU information and/or information systems must include the core security controls. Core security controls typically apply to: • Contracts to an individual (e.g., expert witness, appraiser), • Contracts of 1 year or less duration, inclusive of all options, or • Contracts valued at or less than the SAT, inclusive of all options. Other conditions and factors determine the need for additional security controls.	**C**ore (C) + > **S**implified **A**cquisition **T**hreshold (SAT) = **CSAT** Contracting actions for services that involve contractor access to SBU information and/or information systems, by any contractor (individual or business concern), that are valued above the SAT, inclusive of all options, irrespective of the duration of the contract, must include both the core security controls, and CSAT security controls. Other conditions and factors determine the need for additional security controls.
Core (C) + **Soft**ware Application Development or Maintenance (SOFT) = **CSOFT** Contracting actions for services that involve contractor access to SBU information and/or information systems, by any contractor (individual or business concern) that entails software application development, maintenance, or related support service, regardless of dollar value, and irrespective of the duration of the contract, must include the core security controls, and CSOFT security controls. Other conditions and factors determine the need for additional security controls.	**C**ore (C) + **N**etworked **I**nformation **T**echnology Infrastructure (NET) = **CNET** Contracting actions for services that involve contractor access to SBU information and/or information systems, by any contractor (individual or business concern) that has a networked IT infrastructure (in short, an interconnected group of information systems linked by the various parts of a telecommunications architecture), regardless of dollar value, and irrespective of the duration of the contract, must include the core security controls, and CNET security controls. Other conditions and factors determine the need for additional security controls.

Figure 2: Security Control Level Matrix (By Default Operators)

Time and Dollar Value	Operating Environment or Activity: Standalone, Single, Individual PC User *(No Network)*	Standalone, Single or Multiple PC Users *(No Network)*	Network Environment *(Single or Multiple Users)*	Software Development, Maintenance, or Related Services. *(Single or Multiple Users)*
≤ SAT (inclusive of the value of all options)	C	C	CNET	CSOFT
> SAT (inclusive of the value of all options)	CSAT	CSAT	CNET	CSOFT
≤ 1 Year Contract Duration (inclusive of all options)	C	C	CNET	CSOFT
> 1 Year Contract Duration (inclusive of all options)	CSAT	CSAT	CNET	CSOFT

Table 8: Security Controls Table

NIST CONTROL	**C**ore Security Controls = **C**	**C**ore (C) + > **S**implified **A**cquisition **T**hreshold (SAT) = **CSAT**	**C**ore (C) + **N**etworked **I**nformation **T**echnology Infrastructure (NET) = **CNET**	**C**ore (C) + **Soft**ware Application Development or Maintenance (SOFT) = **CSOFT**
AC-1 Access Control Policy and Procedures			X	X
AC-2 Account Management		X	X	X
AC-3 Access Enforcement		X	X	X
AC-4 Information Flow Enforcement			X	X
AC-5 Separation of Duties			X	X
AC-6 Least Privilege			X	X
AC-7 Unsuccessful Login Attempts		X	X	X
AC-8 System Use Notification		X	X	X
AC-11 Session Lock	X	X	X	X
AC-12 Session Termination	X	X	X	X
AC-14 Permitted Actions without Identification or Authentication			X	X
AC-17 Remote Access			X	X
AC-18 Wireless Access	X	X	X	X
AC-19 Access Control for Mobile Devices	X	X	X	X
AC-20 Use of External Information Systems	X	X	X	X
AC-21 Information Sharing	X	X	X	X
AC-22 Publicly Accessible Content		X	X	X
AT-1 Security Awareness and Training Policy and Procedures			X	X
AT-2 Security Awareness	X	X	X	X
AT-3 Role Based			X	X

NIST CONTROL	**C**ore Security Controls = **C**	**C**ore (C) + > **S**implified **A**cquisition **T**hreshold (SAT) = **CSAT**	**C**ore (C) + **N**etworked **I**nformation **T**echnology Infrastructure (NET) = **CNET**	**C**ore (C) + **Soft**ware Application Development or Maintenance (SOFT) = **CSOFT**
Security Training				
AT-4 Security Training Records			X	X
AU-1 Audit and Accountability Policy and Procedures			X	X
AU-2 Auditable Events	X	X	X	X
AU-3 Content of Audit Records		X	X	X
AU-4 Audit Storage Capacity			X	X
AU-5 Response to Audit Processing Failures			X	X
AU-6 Audit Review, Analysis, and Reporting		X	X	X
AU-7 Audit Reduction and Report Generation			X	X
AU-8 Time Stamps			X	X
AU-9 Protection of Audit Information		X	X	X
AU-11 Audit Record Retention			X	X
AU-12 Audit Generation			X	X
CA-1 Security Assessment and Authorization Policies and Procedures				X
CA-2 Security Assessments				X
CA-3 Information System Connections			X	X
CA-5 Plan of Action and Milestones			X	X
CA-6 Security Authorization			X	X
CA-7 Continuous Monitoring			X	X

NIST CONTROL	**C**ore Security Controls = **C**	**C**ore (C) + > **S**implified **A**cquisition **T**hreshold (SAT) = **CSAT**	**C**ore (C) + **N**etworked **I**nformation **T**echnology Infrastructure (NET) = **CNET**	**C**ore (C) + **Soft**ware Application Development or Maintenance (SOFT) = **CSOFT**
CA-9 Internal System Connections			X	X
CM-1 Configuration Management Policy and Procedures			X	X
CM-2 Baseline Configuration	X	X	X	X
CM-3 Configuration Change Control		X	X	X
CM-4 Security Impact Analysis			X	X
CM-5 Access Restrictions for Change			X	X
CM-6 Configuration Settings	X	X	X	X
CM-7 Least Functionality			X	X
CM-8 Information System Component Inventory	X	X	X	X
CM-9 Configuration Management Plan			X	X
CM-10 Software Usage Restrictions		X	X	X
CM-11 User-Installed Software		X	X	X
CP-1 Contingency Planning Policy and Procedures			X	X
CP-2 Contingency Plan	X	X	X	X
CP-3 Contingency Training			X	X
CP-4 Contingency Plan Testing and Exercises			X	X
CP-6 Alternate Storage Site			X	X
CP-7 Alternate Processing Site			X	X

NIST CONTROL	**C**ore Security Controls = **C**	**C**ore (C) + > **S**implified **A**cquisition **T**hreshold (SAT) = **CSAT**	**C**ore (C) + **N**etworked **I**nformation **T**echnology Infrastructure (NET) = **CNET**	**C**ore (C) + **Soft**ware Application Development or Maintenance (SOFT) = **CSOFT**
CP-8 Telecommunications Services			X	X
CP-9 Information System Backup	X	X	X	X
CP-10 Information System Recovery and Reconstitution			X	X
IA-1 Identification and Authentication Policy and Procedures			X	X
IA-2 Identification and Authentication (Organizational Users)	X	X	X	X
IA-3 Device Identification and Authentication			X	X
IA-4 Identifier Management	X	X	X	X
IA-5 Authenticator Management			X	X
IA-6 Authenticator Feedback		X	X	X
IA-7 Cryptographic Module Authentication		X	X	X
IA-8 Identification and Authentication (Non-Organizational Users)		X	X	X
IR-1 Incident Response Policy and Procedures			X	X
IR-2 Incident Response Training			X	X
IR-3 Incident Response Testing and Exercises			X	X
IR-4 Incident Handling		X	X	X
IR-5 Incident Monitoring			X	X
IR-6 Incident Reporting	X	X	X	X
IR-7 Incident Response			X	X

NIST CONTROL	**C**ore Security Controls = **C**	**C**ore (C) + > **S**implified **A**cquisition **T**hreshold (SAT) = **CSAT**	**C**ore (C) + **N**etworked **I**nformation **T**echnology Infrastructure (NET) = **CNET**	**C**ore (C) + **Soft**ware Application Development or Maintenance (SOFT) = **CSOFT**
Assistance				
IR-8 Incident Response Plan			X	X
MA-1 System Maintenance Policy and Procedures			X	X
MA-2 Controlled Maintenance		X	X	X
MA-3 Maintenance Tools			X	X
MA-4 Non-Local Maintenance	X	X	X	X
MA-5 Maintenance Personnel	X	X	X	X
MA-6 Timely Maintenance			X	X
MP-1 Media Protection Policy and Procedures			X	X
MP-2 Media Access		X	X	X
MP-3 Media Marking			X	X
MP-4 Media Storage	X	X	X	X
MP-5 Media Transport	X	X	X	X
MP-6 Media Sanitization	X	X	X	X
MP-7 Media Use			X	X
PE-1 Physical and Environmental Protection Policy and Procedures	X	X	X	X
PE-2 Physical Access Authorizations		X	X	X
PE-3 Physical Access Control	X	X	X	X
PE-4 Access Control for Transmission Medium		X	X	X
PE-5 Access Control for Output Devices		X	X	X
PE-6 Monitoring Physical Access		X	X	X

NIST CONTROL	**C**ore Security Controls = **C**	**C**ore (C) + > **S**implified **A**cquisition **T**hreshold (SAT) = **CSAT**	**C**ore (C) + **N**etworked **I**nformation **T**echnology Infrastructure (NET) = **CNET**	**C**ore (C) + **Soft**ware Application Development or Maintenance (SOFT) = **CSOFT**
PE-8 Access Records		X	X	X
PE-9 Power Equipment and Power Cabling		X	X	X
PE-10 Emergency Shutoff		X	X	X
PE-11 Emergency Power		X	X	X
PE-12 Emergency Lighting		X	X	X
PE-13 Fire Protection	X	X	X	X
PE-14 Temperature and Humidity Controls		X	X	X
PE-15 Water Damage Protection	X	X	X	X
PE-16 Delivery and Removal		X	X	X
PE-17 Alternate Work Site	X	X	X	X
PE-18 Location of Information System Components	X	X	X	X
PL-1 Security Planning Policy and Procedures			X	X
PL-2 System Security Plan		X	X	X
PL-4 Rules of Behavior		X	X	X
PL-8 Information Security Architecture		X	X	X
PS-1 Personnel Security Policy and Procedures			X	X
PS-2 Position Categorization			X	X
PS-3 Personnel Screening	X	X	X	X
PS-4 Personnel Termination		X	X	X
PS-5 Personnel Transfer		X	X	X
PS-6 Access		X	X	X

NIST CONTROL	**C**ore Security Controls = **C**	**C**ore (C) + > **S**implified **A**cquisition **T**hreshold (SAT) = **CSAT**	**C**ore (C) + **N**etworked **I**nformation **T**echnology Infrastructure (NET) = **CNET**	**C**ore (C) + **Soft**ware Application Development or Maintenance (SOFT) = **CSOFT**
Agreements				
PS-7 Third-Party Personnel Security		X	X	X
PS-8 Personnel Sanctions		X	X	X
RA-1 Risk Assessment Policy & Procedures			X	X
RA-2 Security Categorization			X	X
RA-3 Risk Assessment			X	X
RA-5 Vulnerability Scanning	X	X	X	X
SA-1 System and Security Acquisition Policy and Procedures			X	X
SA-2 Allocation of Resources			X	X
SA-3 Life Cycle Support			X	X
SA-4 Acquisitions		X	X	X
SA-5 Information System Documentation				X
SA-8 Security Engineering Principles				X
SA-9 External Information System Services			X	X
SA-10 Developer Configuration Management				X
SA-11 Developer Security Testing and Evaluation				X
SC-1 System and Communications Protection Policy and Procedures			X	X
SC-2 Application				X

NIST CONTROL	**C**ore Security Controls = **C**	**C**ore (C) + > **S**implified **A**cquisition **T**hreshold (SAT) = **CSAT**	**C**ore (C) + **N**etworked **I**nformation **T**echnology Infrastructure (NET) = **CNET**	**C**ore (C) + **Soft**ware Application Development or Maintenance (SOFT) = **CSOFT**
Partitioning				
SC-4 Information in Shared Resources				X
SC-5 Denial of Service Protection			X	X
SC-7 Boundary Protection			X	X
SC-8 Transmission Confidentiality and Integrity			X	X
SC-10 Network Disconnect			X	X
SC-12 Cryptographic Key Establishment and Management			X	X
SC-13 Use of Cryptography	X	X	X	X
SC-15 Collaborative Computing Devices				X
SC-17 Public Key Infrastructure Certificates			X	X
SC-18 Mobile Code				X
SC-19 Voice Over Internet Protocol			X	X
SC-20 Secure Name/Address Resolution Service (Authoritative Source)			X	X
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)			X	X
SC-22 Architecture & Provisioning for Name/Address			X	X

NIST CONTROL	**C**ore Security Controls = **C**	**C**ore (C) + > **S**implified **A**cquisition **T**hreshold (SAT) = **CSAT**	**C**ore (C) + **N**etworked **I**nformation **T**echnology Infrastructure (NET) = **CNET**	**C**ore (C) + **Soft**ware Application Development or Maintenance (SOFT) = **CSOFT**
Resolution Service				
SC-23 Session Authenticity			X	X
SC-28 Protection of Information at Rest			X	X
SC-39 Process Isolation				X
SI-1 System and Information Integrity Policy and Procedures			X	X
SI-2 Flaw Remediation				X
SI-3 Malicious Code Protection	X	X	X	X
SI-4 Information System Monitoring			X	X
SI-5 Security Alerts, Advisories, and Directives			X	X
SI-7 Software and Information Integrity				X
SI-8 Spam Protection			X	X
SI-9 Information Input Restrictions				X
SI-10 Information Input Validation				X
SI-11 Error Handling				X
SI-12 Information Output Handling and Retention	X	X	X	X
SI-16 Memory Protection			X	X
Privacy Controls				
AR-3 Privacy Requirements for Contractors and Service Providers	X	X	X	X
AR-5 Privacy Awareness and Training	X	X	X	X
DM-2 Data Retention and Disposal	X	X	X	X

NIST CONTROL	**C**ore Security Controls = **C**	**C**ore (C) + > **S**implified **A**cquisition **T**hreshold (SAT) = **CSAT**	**C**ore (C) + **N**etworked **I**nformation **T**echnology Infrastructure (NET) = **CNET**	**C**ore (C) + **Soft**ware Application Development or Maintenance (SOFT) = **CSOFT**
DM-2 Minimization of PII used in Testing, Training, and Research	X	X	X	X
SE-1 Inventory of Personally Identifiable Information	X	X	X	X
SE-2 Privacy Incident Reponses	X	X	X	X

APPENDIX D: PHYSICAL ACCESS CONTROL GUIDELINES

Locked Container

A lockable container is a commercially available or prefabricated metal cabinet or box with riveted or welded seams or metal desks with lockable drawers. The lock mechanism shall be either a built-in key or a hasp and lock. A hasp is a hinged metal fastening attached to the cabinet, drawer, etc. that is held in place by a pin or padlock.

The term container includes all file cabinets (both vertical and lateral), safes, supply cabinets, open and closed shelving or desk and credenza drawers, carts, or any other piece of office equipment designed for storing files, documents, papers, or equipment. Some of these containers are designed for storage only and do not provide protection (e.g., open shelving). For purposes of providing protection, containers can be grouped into three (3) general categories: locked containers, security containers, and safes or vaults.

Security Containers

Security containers are metal containers that are lockable and have a tested resistance to penetration. To maintain the integrity of the security container, key locks shall have only two (2) keys and strict control of the keys is mandatory; combinations shall be given only to those individuals who have a need to access the container. Security containers include the following:

- Metal lateral key lock files,
- Metal lateral files equipped with lock bars on both sides and secured with security padlocks,
- Metal pull drawer cabinets with center or off-center lock bars secured by security padlocks, and
- Key lock “Mini Safes” properly mounted with appropriate key control.

If the central core of a security container lock is replaced with a non-security lock core, then the container no longer qualifies as a security container.

Locks

The lock is the most accepted and widely used security device for protecting installations and activities, personnel information, tax information, classified material, and government and personal property. All containers, rooms, buildings, and facilities containing vulnerable or sensitive items shall be locked when not in actual use. However, regardless of their quality or cost, locks shall be considered as delay devices only and not complete deterrents. Therefore, the locking information system shall be planned and used in conjunction with other security measures. A quarterly inspection shall be made on all locks to determine each locking mechanism’s effectiveness, to detect tampering and to make replacement when necessary.

Access to a locked area, room, or container can be controlled only if the key or combination is controlled. Compromising a combination or losing a key negates the security provided by that lock. Combinations to locks shall have four (4) digits and be changed when an employee who knows the combination retires, terminates employment, transfers to another position, or at least once a year.

Combinations shall be given only to those who have a need to have access to the area, room, or container and shall never be written on a calendar pad, desk blotters, or any other item (even though it is carried on one (1)'s person or hidden from view). Contractor management or designated employee shall maintain combinations for door locks, safes, vaults, or other storage devices. An envelope containing the combination shall be secured in a container with the same or a higher security classification as the highest classification of the material authorized for storage in the container or area the lock secures.

Keys shall be issued only to individuals having a need to access an area, room, or container. An inventory shall be made of all keys made and keys issued. An annual reconciliation shall be done on all key records.

Safes/Vaults

A safe is a General Services Administration (GSA)-approved container of Class I, IV, or V, or Underwriters Laboratories (UL) Listing of TRTL-30, TRTL-60. A vault is a hardened room with typical construction of reinforced concrete floors, walls, and ceilings, uses UL-approved vault doors, and meets GSA specifications.

Secured Interior/Secured Perimeter

Secured areas are internal areas that have been designed to prevent undetected entry by unauthorized contractor employees/persons without an IRS approved interim or final background investigation during duty and non-duty hours.

Access to containers containing SBUs shall be restricted to employees who have an IRS approved background investigation. Secured perimeter/secured area shall meet the following minimum standards:

- This area shall be enclosed by slab-to-slab walls constructed of approved materials, and supplemented by periodic inspection or other approved protection methods, or any lesser type partition supplemented by UL-approved electronic intrusion detection and fire detection information systems. There shall be a manual fire alarm and evacuation system with pull boxes at each door leading out of any encapsulated areas used within the facilities.
  - Unless electronic intrusion detection devices are used, all doors entering the space shall be locked, and strict key or combination control shall be exercised.
  - In the case of a fence and gate, the fence shall have intrusion detection devices or be continually guarded, and the gate shall be either guarded or locked and have intrusion alarms.

- The space shall be cleaned during duty hours in the presence of a regularly assigned employee.
- If there are louvers or vents within the secured area, such as near the door, ceiling, etc. these must be protected to detect and deter unauthorized access to the room/area, using Intrusion Detection System (IDS) methods.
- The contractor shall develop a clean desk policy that requires all employees to secure SBU information after work hours, during extended absence from work such as lunch, or when employee is not immediately working with the SBU information. The clean desk policy must be communicated to all employees.

Restricted / Limited Access Areas

When designating an area as limited access, it is important to ensure that management controls of the area are in place. Examples of a restricted/limited access area include but are not limited to computer rooms, telecommunication closets, processing work areas, or other areas that information is readily available to any employee working within that area.

Using restricted/limited access areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized access and/or disclosure of SBU information.

The contractor shall control all access points to the restricted/limited area. The entry control monitor shall verify the identity of visitors by comparing the name and signature entered in the register with the name and signature of some type of photo identification card, such as a driver's license. When leaving the area, the entry control monitor or escort shall enter the visitor's time of departure. Each restricted area register shall be closed out at the end of each month and reviewed by the area supervisor/manager.

Whenever visitors enter the area, the contractor shall capture the following information: their name, signature, assigned work area, escort, purpose of entry, and time and date of entry.

The contractor escorts visitors and monitors visitor activity, when required.
When unescorted, a restricted/limited access area register shall be maintained at a designated entrance to the restricted area and all visitors (persons not assigned to the area) entering the area shall be directed to the designated entrance.

To facilitate the entry of contractor employees who have a frequent and continuing need to enter a restricted area, but are not assigned to the area, an Authorized Access List (AAL) can be maintained. Each month, a new AAL shall be posted at the front desk and visitors shall be required to sign and the monitor shall not be required to make an entry in the Restricted Area Register. If there is any doubt on the identity of the individual prior to permitting entry, the entry control clerk shall verify the identity prior to permitting entry.

Management or the designee shall maintain an authorized list of all contractor employees with an IRS approved interim or final background investigation that have access to information systems or areas, where SBU information is stored or processed. In addition, the site shall issue appropriate authorization credentials. This shall not apply to those areas within the facility officially designated as publicly accessible.

It is recommended that a second level of management review the register. Each register review shall include a review of the need for continued access, for the employee.

Key Points:

- The area must have physical construction to enable a restricted and/or limited access area, e.g. doors to prohibit unrestricted entry, construction to prevent employees from being able to access room through windows, partitioned walls, etc. Doors that provide access to restricted or protected areas must have either internal door hinges or hinges that are tamper-resistant.

- Restricted/limited access areas shall have signs prominently posted as "Restricted Area" and separated from other areas by physical barriers which will control access. The number of entrances will be kept to a minimum and each entrance controlled. Adequate control will be provided by locating the desk of a responsible employee at the entrance to assure that only authorized persons, with an official need enter. Only individuals assigned to the area will be provided Restricted/Limited Area Access.

- A restricted/limited access area register will be maintained at the main entrance of each restricted area, and all visitors will be directed to the main entrance. Each person entering a restricted area, who is not assigned to the area, will be required to sign the register.
    - The restricted area monitor (staff) will complete the register by adding the individual's name, assigned work area, person to be contacted, purpose for entry, access card number, and time and date of entry.
    - The monitor will identify each visitor by comparing the name and signature entered in the register with the name and signature on some type of photo identification card (i.e. governments issued ID, driver's license) upon verification of identity, the visitor will be issued an appropriate Restricted Area access card.
    - Entry must be approved by the supervisor responsible for the area. Prior to exiting the area the visitor will return the access card to the monitor. The monitor will enter the departure time in the register.

- Each Restricted/Limited Access Area Register will be closed out at the end of each month, reviewed by the restricted area first line supervisor and forwarded to their manager. The manager will review the register and retain it for at least one (1) year. The managerial review is designed to ensure that only authorized individuals with an official need have access to the restricted areas.

- To facilitate the entry of employees who have a frequent and continuing need to enter a restricted area, an Authorize Access List shall be maintained.
    - Individuals whose names appear on the Authorized Access List will not be required to sign-in, nor will the control clerk be required to make any entry in the Restricted/Limited Access Area Register.

These individuals are required to maintain an identifier on the badge that allows the restricted access to be easily recognized, e.g. a different color background on the badge or similar mechanism.

Locking Systems for Restricted Areas

Minimum requirements for locking information systems for secured areas and security rooms are high security pin-tumbler cylinder locks that meet the following requirements:

- Key-operated mortised or rim-mounted high security dead bolt lock,
- A dead bolt throw of one (1) inch or longer,
- Double cylinder design. Cylinders are to have five (5) or more pin tumblers, and
- Hardened inserts or be made of steel if bolt is visible when locked.

Both the key and the lock shall be adequately controlled. Convenience type locking devices such as card keys, sequenced button activated locks used in conjunction with electric strikes, etc., are authorized for use only during duty hours. Keys to secured areas not in the personal custody of an authorized employee and any combinations shall be stored in a security container. The number of keys or persons with knowledge of the combination to a secured area shall be kept to a minimum. Keys and combinations shall be given only to those individuals, preferably supervisors, who have a frequent need to access the area after duty hours. Electronic access control systems with afterhours alarming capability can be used to secure doors to secure areas after duty hours.

Mail Processing

If IRS mail is received, the contractor shall ensure that IRS incoming mail be stored in a secured area, i.e. in locked containers.

Data Center Controls

The primary room must be a secured room/space is one (1) that meets the following security requirements:

Space must be enclosed by slab-to-slab walls, which reach structural floor to structural ceiling, constructed of approved materials (normal construction material, permanent in nature such as masonry brick or drywall), that would prevent easy penetration/compromise.

If walls are not structural floor to structural ceiling, the use of wire mesh or woven wire fabric at least 10-gauge chain link fence installed above ceiling and/or under the floor to

prevent unauthorized entry; or use of IDS (motion sensors) above ceiling or beneath floor to prevent unauthorized entry, is acceptable.

When IDS are used, procedures shall be in place requiring that response time to alarms be 15 minutes or less.

Equipment and utilities must be locked to prevent tampering by unauthorized personnel. These keys will be controlled and limited to authorized employees. Non-IRS controls and activities must not be collocated in these rooms.

Placement of cameras is largely driven by risk or potential risk. High risk areas must be effectively covered and include the following areas:

Access to data centers shall be controlled using biometric devices, or other form using two factor authentication.

Doors: Doors that permit access (e.g., ingress/egress) to the exterior must be covered by interior cameras. Interior doors that permit access to other interior controlled areas must capture the facial view of persons as they enter and leave the space.

Controlled Rooms: Fixed camera coverage of areas such as secured storage rooms, computer rooms, security system control rooms, and main utility closets. Camera placement and coverage must be designed and monitored so equipment, storage goods, and/or design does not interfere, diminish or block surveillance.

The contractor must control all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls to the areas officially designated as publicly accessible, as appropriate, in accordance with the lockbox's assessment of risk. This requirement applies to both employees and visitors.

The contractor must meet and control physical access to information system devices that display information to prevent unauthorized individuals from observing the display output. (Reference PE-5)

The contractor must monitor physical access to the information system to detect and respond to physical security incidents. (Reference PE-6)

Access logs must be maintained to identify visitors to the computer room facilities. The log must include: name & organization of the person visiting; signature of the visitor; date of access; time of entry and departure, purpose of visit. Designated officials must review logs periodically. (Reference PE-8)

The contractors must control information system-related items, including hardware, firmware, software, from entering and exiting the facility and maintain appropriate records of these items. (Reference PE-16)

Contractor employees must not process and/or store Federal Tax Information (FTI) at any sites, other than IRS approved contractor sites. Information must not be processed and/or stored from any employee's temporary and/or permanent residence, e.g. via home office or telecommuting. (Reference PE-17)

Floor lifting devices shall be mounted immediately adjacent to each portable fire extinguisher and readily available.

Data Center Fire/Environmental Conditions

The contractor shall install a firewall to separate the main doors to computer areas and adjacent tape or other storage libraries, as necessary to protect large volumes of media.

The contractor must control physical access to information systems telecommunications service, distribution, and or network lines within the facility that would inhibit unauthorized access, interception or damage. (Reference PE-4)

There shall be an audible sounding device (alarm) that reports to a central receiving point for action/response, for each room within the firewall encapsulated area of the computer complex that will alert the complex that unauthorized person(s) have entered the area.

Whenever multiple devices are being tracked for any activation and/or incidents, each device shall annunciate separately to the on-site protection console.

There shall be a one (1) hour fire resistive separation of the computer (electronic equipment) area perimeter from adjoining areas to protect the electronic equipment from the damaging effects of a fire which may occur outside the equipment area.

There shall be an approved Ionization system in each computer room/tape library and ionization detector heads installed above suspended ceilings (unless ceiling is fire rated), on suspended ceilings and below elevated floors, scaled to the size of the facility being safeguarded.

The contractor must protect power equipment and power cabling for the information system from damage and destruction. (Reference PE-9)

As occupants of the contractor, the contractor must comply with all federal, state and local codes including but not limited to National Fire Protection Association (NFPA) and National Electrical Code (NEC) requirements. Upon request, the contractor must be able to present the certification of compliance for each site. (Reference PE-10)

The contractor must provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system, in the event of a primary power source loss. (Reference PE–11)

The contractor must employ automatic emergency lighting of computer room facilities in the event of a power outage or disruption and that cover emergency exits and evacuation routes. (Reference PE-12)

The contractors must employ and maintain fire suppression equipment and detection equipment that can be activated in the event of a fire. (Reference PE-13)

In addition, contractors shall ensure there are systems in place to continuously monitor all electronic detection, extinguishing, and environmental and utility support systems to detect abnormal conditions.

The contractor shall install separately contained/valve wet pipe, water sprinkler system (pipe scheduled or hydraulically designed type) inside the entire firewall, encapsulated computer room and tape library areas with automatic power cut--off capability. (National Fire Protection Association (NFPA) Standard No. 13 provides details on installation of acceptable sprinkler systems).

The contractors must regularly maintain, within acceptable levels, and monitor, the temperature and humidity within computer room and telecommunication facilities containing information systems and assets. (Reference PE-14).

All air conditioning and ventilating systems must be in compliance with Section 301 of RP--1 and NFPA Standard No. 90A to ensure that the systems are designed to prevent the spread of fire, smoke and fumes from exposed areas into the computer room or tape library.

Sprinkler water flows shall contain alarms and supply valve controls.

There are Floor drains or sump pumps to provide water drainage in the event of a sprinkler head activation or a plumbing leak above the ceiling or under the floor.

There is a Sprinkler shut--off valve (also called OS&Y) that controls the sprinkler system to the computer and/or library.

The contractors must protect the information systems from water damage resulting from broken plumbing lines or other sources of water by ensuring that master shutoff valves are accessible, working, and known to key personnel. (Reference PE-15)

The information systems must be placed to minimize damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. (Reference PE-18)

APPENDIX E: REFERENCE

Computer Security Act of 1987
http://csrc.nist.gov/groups/SMA/ispab/documents/csa_87.txt

Federal Acquisition Regulation Part 2, refer to
http://www.gpo.gov/fdsys/pkg/CFR-2011-title48-vol1/pdf/CFR-2011-title48-vol1-sec2-101.pdf

Federal Information Security Management Act, refer to
http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

Federal Information Processing Standards 140-2, Security Requirements for Cryptographic Modules, refer to
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Federal Information Processing Standards 199, Standards for Security Categorization of Federal Information and Information Systems, refer to
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Federal Information Processing Standards 200, Minimum Security Requirements for Federal and Information Systems, refer to
http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Federal Trade Commission Financial Privacy Rule and Safeguards Rule, refer to
http://www.gpo.gov/fdsys/pkg/FR-2000-03-01/pdf/00-4881.pdf

Gramm-Leach Bliley Act, refer to
http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

Internal Revenue Code Section 26 U.S.C. § 6103, refer to
http://www.gpo.gov/fdsys/pkg/USCODE-2011-title26/html/USCODE-2011-title26-subtitleF-chap61-subchapB-sec6103.htm

Internal Revenue Code Section 26 U.S.C. § 7213, refer to
http://www.gpo.gov/fdsys/pkg/USCODE-2010-title26/html/USCODE-2010-title26-subtitleF-chap75-subchapA-partI-sec7213.htm

Internal Revenue Code Section 26 U.S.C. § 7213A, refer to
http://www.gpo.gov/fdsys/pkg/USCODE-2011-title26/html/USCODE-2011-title26-subtitleF-chap75-subchapA-partI-sec7213A.htm

Internal Revenue Code Section 26 U.S.C. § 7431, refer to
http://www.gpo.gov/fdsys/pkg/USCODE-2011-title26/html/USCODE-2011-title26-subtitleF-chap76-subchapB-sec7431.htm

Internal Revenue Manual 10.8.1, Information Technology (IT) Security, Policy and Guidance, refer to
http://www.irs.gov/irm/part10/irm_10-008-001.html

Internal Revenue Manual 10.8.2, Information Technology (IT) Security, IT Security Roles and Responsibilities, refer to
http://www.irs.gov/irm/part10/irm_10-008-002.html#d0e254

National Institute of Standards and Technology Special Publication 800-18 Revision 1, Developing Security Plans for Federal Information Systems, refer to
http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

National Institute of Standards and Technology Special Publication 800-53 (Revision 4), Recommended Security and Privacy Controls for Federal Information Systems and Organizations, refer to
http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

National Institute of Standards and Technology Special Publication 800-88, Guidelines for Media Sanitization, refer to
http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

Office of Management and Budget Memorandum 07-16
http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-16.pdf

Office of Management and Budget Memorandum 08-23:
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf

Office of Management & Budget OMB Circular A-130 – Management of Federal Information Resources, refer to
http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

Privacy Act of 1974, refer to
http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf

Sarbanes-Oxley Act, refer to
http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf

Section 552a of Title 5, United States Code
http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf