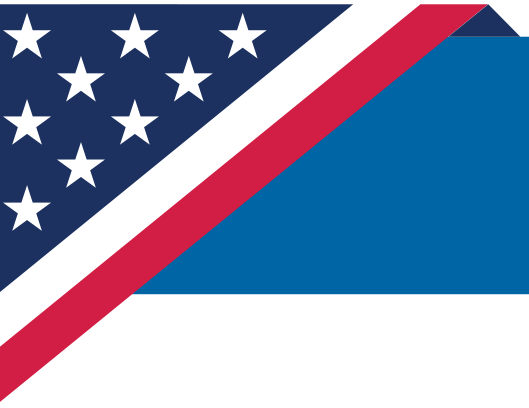

Information Technology

CyberSecurity

Publication 4812

Contractor Security & Privacy Controls

Handling and Protecting Information or Information Systems

This Publication Pertains to IT Assets Owned and Managed at Contractor sites

Highlights of Publication 4812

Publication 4812 identifies security and privacy control requirements for contractors and their subcontractors that have access to or manage Internal Revenue Service (IRS) Sensitive But Unclassified (SBU) data on their own information systems or resources. The level of the required security and privacy controls will vary depending on the duration, size, and complexity of the supported contract.

Publication 4812 defines basic security and privacy control requirements for contractors, subcontractors, contractor employees, and subcontractor employees who will either:

- Have access to, develop, operate, host, or maintain IRS SBU data or information systems for tax administration purposes outside of IRS facilities or outside of the direct control of the Service, and/or
- Have access to, compile, process, transmit or store IRS SBU data 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 (EIT) (as defined in FAR Part 2) to access, compile, process, or store IRS SBU data while working at an IRS owned or controlled facility.

The IRS defines SBU data in IRM 10.5.1.2.2, Sensitive But Unclassified (SBU) Data, as any information which, if lost, stolen, misused, accessed, or altered without proper authorization, may adversely affect the national interest or the conduct of federal programs (including IRS operations), or the privacy to which individuals are entitled under the Privacy Act (5 U.S.C. 552a).

SBU data includes but is not necessarily limited to:

- Federal Tax Information (FTI), Personally Identifiable Information (PII), Protected Health Information (PHI), procurement sensitive information, system vulnerabilities, case selection methodologies, systems information, enforcement procedures, and investigation information. (See Appendix B “Glossary” for definitions).
- Live data, which is defined as production data in use. Live means that when changing the data, it changes in production. The data may be extracted for testing, development, etc., in which case, it is no longer live. Generally, SBU data should not be used for testing or training and non-production systems must maintain the same security and privacy controls which protect live data when SBU data is introduced.

Table of Contents

1.0 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 and privacy protection for "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 and privacy controls/criteria in NIST Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations. NIST provides a series of recommended security and privacy controls to be employed by agencies and service providers to ensure 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 26 U.S.C § 6103, 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.

When entering into a contract with the IRS the contractor agrees to allow the IRS access to their site within 24 hours of notification by the Contracting Officer's Representative (COR) or Contracting Officer (CO). Failure to allow access is considered a breach of contract terms and conditions, which could result in termination of the contract or assessment of liquidated damages as agreed to within FAR clause 52.211-11 -- Liquidated Damages -- Supplies, Services, or Research and Development (Sept 2000).

In signing a contract, the contractor agrees to provide the COR an updated Plan of Actions & Milestones (POA&M) for any open findings identified during an on-site or virtual assessment conducted by the IRS at a minimum quarterly. Failure to provide a POA&M to demonstrate how the contractor is addressing risks is considered to be a breach of contract terms and conditions, which will result in the COR withholding invoice approval until a POA&M is provided.

Refer to CA-5 (Plan of Actions and Milestones) and RA-5 (Vulnerability Monitoring and Scanning) for additional details on POA&M and Vulnerability Scan reporting requirements.

2.0 Purpose

This publication defines basic security and privacy controls, requirements and standards that apply to contractors, subcontractors, contractor employees, and subcontractor employees supporting the primary contract. The information in this publication is based on the security and privacy controls framework under NIST SP 800-53 Rev. 5, where those contractor employees have access to develop, operate, or maintain IRS SBU data. While NIST SP 800-53 Rev. 5, is a general guide, the intent of Publication 4812 is to provide IRS privacy and security requirements specific to 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 IRS SBU data and information systems.

As described in NIST SP 800-53 Rev. 5, "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".

3.0 Scope

The requirements in this publication and the security and privacy controls contained hereinafter are based on NIST SP 800-53 Rev. 5.

3.1. IRS Security and Privacy Controls Structure

NIST provides Federal agencies the flexibility to apply the privacy and security concepts and principles in NIST SP 800-53 Rev. 5 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**,** the IRS identifies security and privacy controls for the organization's information and information systems in the following three key documents:

- Internal Revenue Manual (IRM) 10.8.1 – Information Technology (IT) Security, Policy and Guidance (The public document is redacted.),
- IRM 10.5.1 – Privacy and Information Protection, Privacy Policy (publicly available), and
- Publication 4812 – Contractor Security & Privacy Controls.

While IRM 10.8.1 and Publication 4812 are both based on NIST SP 800-53 Rev. 5, they apply to different operating environments – internal and external to the IRS respectively and 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 procedures to be used by each office, or business operating division, and functional unit within the IRS that uses IRS information systems. This manual 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. 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 (https://www.irs.gov/irm/part10/irm_10-008-001r)

3.1.2 IRM 10.5.1 Applicability

IRM 10.5.1 defines the uniform policies used by IRS personnel and organizations to carry out their responsibilities related to privacy. The IRM establishes the minimum baseline privacy policy and requirements for all IRS SBU data (including PII and FTI). It applies to all offices, business, operating, and functional units within the IRS. It also applies to all IRS personnel, which this IRM defines as including the following categories: individuals and organizations having contractual arrangements with the IRS, including employees, seasonal/temporary employees, interns, detailed individuals, contractors, subcontractors, non-IRS-procured

contractors, vendors, and outsourcing providers, with any access to SBU data. Contractors who need to refer to that document for guidance may access it at: (https://www.irs.gov/irm/part10/irm_10-005-001)

3.1.3 Publication 4812 Applicability

Publication 4812 identifies security and privacy controls specific to IRS contractor's information systems. These controls are based on controls established in NIST SP 800-53 Rev. 5. Publication 4812 contains IRS-specific requirements that meet the standard for NIST SP 800-53 Rev. 5, and the security and privacy 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 Rev. 5. Contractors may, at their discretion, refer to NIST SP 800-53 Rev. 5, to gain a better understanding of the common standards, but shall coordinate with the COR for their contract for clarification on Publication 4812 security and privacy controls/standards or guidance/requirements specific to IRS.

Note: (All NIST Special Publication (800 series) are available at the following web site - https://csrc.nist.gov/publications/sp800.)

Publication 4812 defines basic security and privacy controls, requirements, and standards required of contractors, subcontractors, contractor employees, and subcontractor 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 data on their own information systems or that of a subcontractor, or third-party service provider, that use their own information systems (or that of others) and EIT (as defined in FAR Part 2) to access, compile, process, or store IRS SBU data while working at an IRS owned or controlled facility.

Publication 4812 is incorporated by contract clause into IRS contracts, agreements, and/or task orders (directly or through flow down provisions to subcontractors). IRS IT Security/FISMA requirements language is also included in any solicitations/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. The most up-to-date Publication 4812 is applicable to the contractor and is available on the IRS public website.

As used in this publication, the term "contract" unless specified otherwise, includes 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 contract, order, or agreement. This publication may also be used and incorporated into interagency agreements in which IRS is the requesting agency and the servicing agency does not have guidelines (or security controls consistent with NIST SP 800-53 Rev. 5 in place comparable to Publication 4812).

As described in greater detail in subsequent sections, there are two baseline levels of security controls, networked environments, and software development. The specific security and privacy controls associated with each control level can be found in Publication 4812, Section 8.4, and Appendix C. The use of baseline levels of security and privacy controls notwithstanding, IRS always reserves the right to add other controls to any given contract, order, or agreement 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, in the best interest 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 and privacy controls applicable to any given contracting action subject to Publication 4812.

4.0 SBU Data

The IRS defines Sensitive But Unclassified Information (SBU) Data in IRM 10.5.1.2 as; "*any information which, if lost, stolen, misused, accessed or altered without proper authorization, may adversely affect the national interest or the conduct of federal programs (including IRS operations), or the privacy which individuals are entitled under the Privacy Act" (5 U.S.C. 552a).*

SBU data includes but is not necessarily limited to:

- Federal Tax Information (FTI), Personally Identifiable Information (PII), Protected Health Information (PHI), procurement sensitive information, system vulnerabilities, case selection methodologies, systems information, enforcement procedures, investigation information.
- Live data, which is defined as production data in use. Live means that when changing the data, it changes in production. The data may be extracted for testing, development, etc., in which case, it is no longer live. Live data often contains SBU data.

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

SBU data shall only be released or accessible via access to information systems to those individuals who have been approved for interim/final staff-like access by IRS Personnel Security (see definition of staff-like access in Appendix B). Additionally, they should have a "need to know" to perform the work required under the contract.

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

- Federal Tax Information (FTI)
- Law Enforcement Sensitive (LES) Information,
- Employee information,
- PII, 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 as defined by IRC, 26 U.S.C. § 6103(b).

4.2 Law Enforcement Sensitive (LES) Information

Law enforcement data is often sensitive in nature. This data falls under the data category called Law Enforcement, which includes grand jury, informant, and undercover operations information and procedural guidance.

4.3 Employee Information

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

4.4 Personally Identifiable Information (PII)

As defined in OMB Circular A-130: "Personally Identifiable Information" is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Since there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available – in any medium and from any source – that would make it possible to identify an individual.

4.5 Other Protected Information

Other protected information includes any knowledge or facts received or created by the 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 (FOIA);
- Proprietary data;
- Procurement sensitive data, such as vendor 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;
- Any information, which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission; and
- Information that would disclose techniques or procedures within the IRS not necessarily known to the public.

5.0 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 and privacy controls apply to both information and information systems.

6.0 Unauthorized Access (UNAX) and Disclosure of Information

IRC Section 26 U.S.C. § 7213A makes the unauthorized inspection of returns and return information a misdemeanor punishable by fines, imprisonment, or both. 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.

Disclosure of returns and return information is generally prohibited unless authorized by statute. Returns and return information are defined by IRC, 26 U.S.C. § 6103(b). 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 employees who make unauthorized disclosures of returns and return information. The sanctions of the IRC are designed to protect the privacy of taxpayers.

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 and subcontractors 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 documented notification to employees and subcontractors (at any tier) regarding, the importance of protecting returns and return information. 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, as provided under the IRC are subject to continual assessment and oversight to ensure their adequacy and efficacy.

7.0 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 privacy and security-related clauses and language are included in applicable contracts with assistance from requiring activity and CSA.
- 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 correct or mitigate identified security vulnerabilities.
- Modifies the contract, when risk level requires modification, based upon Cybersecurity recommendations.
- Assists with reporting and mitigation of incidents as appropriate. (See section 18.6 IR-6 Incident Reporting.)

7.1.2 Contracting Officer's Representative (COR)

- Facilitates CSAs and serves as the liaison between the CSA Team and the contractor when scheduling CSAs and by being the primary IRS focal point for the contractor.
- Escalates key information to the CO related to contractor risk.
- Provides at a minimum quarterly status of all related the Plan of Actions and Milestones (POA&M) to Cybersecurity.
- Furnishes the CSA documents 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.
- Ensures all security awareness, privacy, records management, and physical environment mandatory briefings assigned to each contractor are completed, recorded in the learning system, and within the IRS required timeframe for completion.
- Serves as the liaison between Privacy Governmental Liaison and Disclosure (PGLD) and the contractor. If entering into a data sharing agreement with a contractor, or vendor that involves custody of, or access to IRS-held PII that will be collected, maintained, or disseminated using IT, work with the contractor to complete a Privacy Threshold Analysis (PTA) to document and identify any additional privacy compliance requirements. A PTA can be used to determine whether a full Privacy & Civil Liberties Impact Assessment (PCLIA) is needed.

- Ensures (when applicable) the completion or update of a PCLIA in the Privacy Impact Assessment Management System (PIAMS). For any PCLIAs that will expire at the end of the contract, or after three years, whichever comes first, the COR should email *Privacy for instructions on renewing a PCLIA.
- Ensures all contractors and subcontractors with staff-like access to SBU data are properly investigated prior to being given access.
- Assists with reporting and mitigation of incidents as appropriate. (See section 18.6 IR-6 Incident Reporting.)

7.1.3 Contractor Security Assessment Team (CSA)

- Establishes the schedule for CSAs in coordination with COs, CORs, and targeted contractors.
- Conducts on-site or virtual CSAs.
- Coordinates with the COR to identify contractor security review timeframes to conduct assessments.
- Provides the CSA documents to the COR, the CO, and the Security Program Management Office. The CSA documents include:

    1. Executive Memorandum: that includes the contractor IT environment, physical description of the site, and significant security findings;
    2. Findings Report: which is a PDF version of the findings found during the assessment in a tabular format listing the security control, justification for the finding, and recommendation to resolve the issue/finding; and
    3. Data Collection Instrument (DCI) : PDF versions of the DCI completed during the on-site/virtual assessment which detail the observations of the CSA Team.

- Maintains and updates, as appropriate, Publication 4812 and coordinates changes or updates with Procurement and other organizational components and stakeholders.
- Acts as a resource for CORs/ Business Operating Divisions (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).
- Alerts Computer Security Incident Response Center (CSIRC) and/or Situation Awareness Management Center (SAMC) of any potential or suspected incidents, risks, or vulnerabilities discovered in the course of conducting a Contractor Security Assessment that represent 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 while conducting a CSA that falls within each component's areas of responsibility.

7.1.4 Privacy, Governmental Liaison and Disclosure (PGLD)

PGLD is responsible for safeguarding and protecting sensitive taxpayer and employee information while promoting government transparency and accountability through better

access to government information. Questions about privacy can be routed through the COR and sent to *Privacy mailbox if necessary.

To accomplish its mission, PGLD:

- Preserves and enhances public confidence by advocating for the protection and proper use of sensitive information;
- Protects the sensitive information and privacy of taxpayers and IRS employees;
- Reduces vulnerabilities for identity theft, which promotes identity protection;
- Ensures IRS records (hard copy and electronic), including those containing PII, are managed appropriately and in accordance with the Records Control Schedules (RCS) Document 12990 and General Records Schedules (GRS) Document 12829;
- Investigates, analyzes, and resolves incidents involving the loss or theft of an IRS asset, or the loss, theft, destruction, or disclosure of PII;
- Works with all IRS operations to ensure only authorized disclosures and data sharing;
- Partners with federal, state, tribal, territorial and local governmental agencies to promote privacy and protect FTI;
- Exchanges FTI as authorized by law with external stakeholders;
- Safeguards FTI held by data exchange partners;
- Protects IRS employees with cautionary indicators on appropriate taxpayer accounts; and
- Processes requests for agency records requested under the FOIA Title 5 U.S.C 552.

7.1.5 Facilities Management and Security Services (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 the CSA Team to conduct physical security portion of the CSA.

7.1.6 Personnel Security (PS)

- Receives and processes all investigative requests from the COR.
- Responsible for determining eligibility and suitability for all contractor employees who require staff-like access to IRS facilities, systems, or SBU data.
- 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 Designation Tool (PDT) to assign the position risk designation (or make adjustments/updates, as needed) prior to granting contractor personnel interim or final staff-like access to IRS information or information systems.

7.1.7 Project Manager/Task Manager

- The Project Manager/Task Manager is assigned by the Business Unit (BU) and is responsible for the contractor's work as described in the signed contract.
- Coordinates with the contractor to complete any required PTAs and PCLIA within PIAMS.
- Review's findings and collaborates with the contractor to develop a POA&M to correct or remediate identified risks.
- Coordinates with the contractor to update the POA&M and provide updates to the COR, at a minimum quarterly.

7.2 Contractor

To ensure IRS information and information systems are always protected, 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 and privacy 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 Vendor Point of Contact (POC) and alternate Vendor POC to all contracts requiring access to Treasury/Bureau information, information technology and systems, facilities, and/or assets. The Vendor POC is the contractor's primary point of contact for the Government on all privacy and 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.

The contractor is responsible for protecting SBU data (including PII and FTI) based on the contract, the PCLIA, and the privacy and security controls defined in this publication.

7.2.1 Contractor Point of Contact (POC)

Within 10 calendar days of contract award or order issuance, the Contractor POC shall submit to the COR a list of contractor employees who will have a significant role or responsibility for information/IT security in the performance of the contract including those authorized to handle SBU. The Contractor POC 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 data, regardless of location or facility, to include contractors who need such access including the use of other IT resources, at contractor managed facilities.

The Contractor POC is responsible for ensuring the following responsibilities are addressed through the life cycle of the contract:

- At a minimum, quarterly, provide updates to the CO/COR on all identified findings using a POA&M;
- Report all incidents to the IRS, as required under the 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; and
- Ensure all employees take required IRS training annually related to records management and the protection of information.

7.2.2 Contractor Employees

- Ensure all required training is completed annually.
- Ensure all privacy and 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 addresses all aspects of IT security.

7.3.1 Contractor Security Policies and Procedures

Contractors and subcontractor are responsible for developing policies and procedures to implement security controls and requirements, as established by this publication and the contract.

As described in NIST SP 800-53 Rev. 5 the first security control in each family is also known as the "*dash one"* 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 and privacy controls and control enhancements in the family.

A contractor or subcontractor who is subject to the security and privacy 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 control and security control family. For example, if the Personnel Security Policy and Procedures (PS-1) 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 control, as specified in Publication 4812.

Only when the contractor or subcontractor does not have standing policies and procedures that adequately and fully address each respective security control family's dash one 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.

The Vendor POC, in collaboration with the COR, shall ensure all contractor and subcontractor employees performing or proposed to perform under the contract as well as those meeting the definition of the term staff-like access are identified to the IRS at time of the award (or assignment) to initiate appropriate security screening.

Working collaboratively, the Vendor POC, the COR and the CO shall ensure that any personnel who are not favorably adjudicated or otherwise pose a security risk are immediately removed from performing work under contract with the IRS, and suitable replacement personnel agreeable to the IRS are provided.

7.3.3 Contractor Training

Ensure all contractor and subcontractor employees who require staff-like access to IRS information or information systems regardless of their physical location complete the required Security Awareness Training (SAT) prior to being granted access to SBU data.

As of December 2018, the IRS has developed a methodology to assign the following mandatory briefings to all individuals supporting these types of contracts: Annual Cybersecurity Awareness, Privacy, Information Protection & Disclosure (PIPD), Records Management, Insider Threat Awareness, and UNAX.

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.

Reference Section 12.2 AT-2 Literacy Training and Awareness for time requirements to complete training

7.3.4 Contractor Information Protection

Ensure all SBU data is protected at rest, in transit, and in exchanges (i.e., internal and external communications). Limit access to SBU data 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 and subcontractor shall employ encryption concepts and approved standards to ensure the confidentiality, integrity, and availability of the SBU data, consistent with the security controls under Publication 4812 and any security requirements specified elsewhere in the contract.

7.3.5 Rules of Behavior

Contractors and subcontractors shall develop and distribute a set of internal rules of behavior regarding access to and the 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 Rev. 5, shall clearly delineate responsibilities, and expected behavior of all individuals with access to information systems and/or government information and/or IRS SBU data. 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 data. 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 (NDAs), and the completion of all required awareness training.

8.0 Contractor Security Assessments (CSA)

8.1 Overview

Security and privacy 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 or virtual evaluations performed by the IRS to assess and validate the effectiveness of security and privacy 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 additional controls or protections are necessary to protect returns, return information, personal privacy, other SBU data, and organizational assets and operations.

All contracts subject to this publication, may be required to undergo an on-site or virtual CSA annually.

8.2 Types of Assessments

Current contract conditions and the stage of the acquisition lifecycle will dictate the type of Contractor Security Assessment the IRS will perform. Qualifying events or conditions that may prompt or necessitate the IRS to 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 data and/or information systems, and other factors. 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 a contract is awarded.
- Contractor Security Self-Assessment: Upon the direction of IRS Cybersecurity, the contractor shall complete and submit to the COR and concurrently to Cybersecurity an assessment of the contractor's adherence to high-risk controls having significant impact on the availability, confidentiality, and integrity of IRS SBU. Cybersecurity will provide to the contractor via the COR, a questionnaire describing the requirement,

proposed test procedure, determination (Met, Not Met, Not Applicable) and justification for the determination.

- Follow-up Security Assessment: Based upon the magnitude of issues identified on a post-award assessment, a return visit may be warranted to evaluate remedial actions taken to address security issues. This type of review will focus on the open findings and is generally a one-day exercise.
- Periodic Post–Award Assessments: Based upon the type of work being performed and the volume of SBU data 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 intent to conduct an on-site or virtual Contractor Security Assessment. Approximately one month prior to the projected timeframe or proposed date of the assessment, the IRS will coordinate the logistics for the upcoming assessment. 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.

Typically, an on–site or virtual CSA is three days in duration.

8.4 Security Control Levels

Contractor sites and work environments using IT assets to access, process, manage, or store SBU data under contract to the 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, two control sets are categorized (within the assigned moderate impact designation) as follows:

- Networked Information Technology Infrastructure (NET), and
- Software Application Development or Maintenance (SOFT).

Scope: The defined conditions 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, configuration, 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 telecommunication's architecture).

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

Networked Information Technology Infrastructure (NET)

Contracting actions for services that involve contractor access to SBU data 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 telecommunications architecture).

Examples of a networked infrastructure include:

IRS SBU is maintained on a file or shared area, where access controls are used to manage access to the file or shared area; or
IRS SBU 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.

Software Application Development/Maintenance (SOFT)

Contracting actions for services that involve contractor access to SBU data and/or information systems, by any contractor (individual or business concern) that entails software application development, maintenance, configuration, or related support service.

An example of this type of contract or environment includes contractor sites, where multiple employees have access to IRS SBU data 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, configure, and perform information system maintenance or other related support service.

8.5 Scope of Assessments

CSAs typically concentrate on the following key areas:

- Information and information systems;
- The physical environment in which the information system or systems resides, and/or where the information is handled, or processed;
- Personnel who have access to, or are responsible for the handling or processing of information and information systems;
- Evaluation of all applicable Publication 4812 security and privacy controls;
- Verification of all personnel security background investigations or interim/final staff-like access determinations for all contractor employees working on the IRS contract, including subcontractor employees, and IT support personnel (at any tier) who have unescorted staff-like access to IRS facilities, SBU data, or information systems;
- Validation of IT security configurations including, but not limited to, workstations, servers, routers, and switches;

- Verification of employee's completion of IRS mandated SAT, which is based on the completion of various information protection briefings (on an annual basis) on information system security, disclosure, privacy, physical security, and/or UNAX – commensurate with the assigned risk designations of the position for the work being performed and the category of SBU data to which the employee has access;
- Vulnerability and configuration (compliance) scans; and
- Preliminary identification of any weaknesses, threats, or vulnerabilities, with more details to be provided in CSA documents at a later date.

8.5.1 Collaboration on Contractor Security Assessment

8.5.1.1 Before the Assessment

Contractors shall coordinate with the IRS on all aspects of preparation for the assessment to including, but not limited to agreement on time and places of assessment, timely submission of any pre-site visit materials, as requested, making ready for inspection, all other policies, documentation, and records that shall be needed at the time of 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 protect against threats and hazards to the security, confidentiality, integrity, and availability of IRS data.

Access to contractor facilities and IRS information and/or information systems by IRS representatives (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 (PIV) card. PII such as a Social Security number (SSN) or date of birth (DoB) shall not be requested of government personnel conducting an assessment.

A contractor facility that maintains classified information, is subject to the National Industrial Security Program, and 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 60 days of the completion of the CSA, the CSA Team shall furnish to the CO/COR the final CSA documents.

The CSA documents contain the results of the security assessment. This typically includes:

- Findings of "not met" or "repeat not met" (with respect to not meeting individual security controls standards/requirements);

- Identifying the parts of the security controls that did not produce a satisfactory result, or may have the potential to compromise IRS information, or the contractor's information system;
- An evaluation 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; and
- Recommendations for correcting deficiencies in the security controls and reducing or eliminating identified vulnerabilities.

The Findings Report 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 CSA and delineates the tasks necessary to correct, remediate, or mitigate less than satisfactory findings.

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 Findings Report. The contractor shall track and furnish IRS status or progress reports, as directed.

8.5.2 Continuous Monitoring of Security and Privacy 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.

9.0 Privacy and Information Protection

9.1 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 Rev. 5, in combination, help ensure that appropriate security requirements and controls are applied to all federal information and information systems.

As required by FIPS 199, organizations use the security categorization results to designate information systems as low-impact, moderate-impact, or high-impact.

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 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 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, one or more 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.)

10.0 Security and Privacy Control Organization and Structure

This document provides required controls for protecting SBU data, developed from NIST guidance. The security controls in this document are organized into families as described in NIST SP 800-53 Rev. 5. Each security control family contains security controls related to the functionality of the family. A two-character, unique identifier is assigned to each security control family.

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

Table 1: NIST Families of Security and Privacy Controls

IDENTIFIER	FAMILY
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Assessment, Authorization, and Monitoring
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
PT	PII Processing and Transparency
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
SR	Supply Chain Risk Management

The twenty security control families in NIST SP 800-53 Rev. 5 are closely aligned with the seventeen minimum security requirements for federal information and information systems in FIPS 200. One additional family, Program Management (PM) provides controls for information security programs. PM, while not referenced in FIPS 200, provides security and privacy controls at the organizational level rather than the information system level. The PM controls address the strategic level implementation of an overall security and privacy program. Contractors subject to Publication 4812 are not responsible for the implementation of IRS strategic security PM but are required to abide by PM Privacy controls in Publication 4812.

11.0 Access Control (AC)

The AC family provides security controls required to restrict access to IRS SBU data and information systems. IRS SBU data shall be restricted to those contractors and subcontractors who have been approved for interim/final staff-like access by IRS Personnel Security, and have a "need-to-know".

11.1 AC-1 Access Control Policy and Procedures

For all contractors and subcontractors who have IT assets (i.e., information systems or servers) the contractor and subcontractor shall designate an official to manage the development, documentation, and dissemination of the access control policies and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organizational Entities; and
- Compliance.

Contractors and subcontractors shall review/update those policies and procedures every three years 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 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 unique account created and used for each employee who shall perform IRS work on that asset.

Employees who perform privileged roles such as System Administrators (SA) shall have two user accounts: one for privileged duties and one for general user activity.

a. Each account shall be independent of the other, be limited in use, and shall be used solely for its defined purpose. For example, a SA shall not use the SA account to access the employee's own personal files.
b. Service accounts have specific purposes and shall not be used otherwise.

There shall be a procedure that describes how 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 and subcontractor shall notify account managers:

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

The contractor shall support the management of system accounts using automated mechanisms. Automated mechanisms include helpdesk software, email, telephonic, and text messaging notifications. The information system shall automatically remove/terminate temporary and emergency accounts after two business days.

The information system shall automatically disable user accounts after 120 days of inactivity. The information system shall automatically disable administrator accounts after 60 days of inactivity. The contractor shall disable accounts within the information system when the accounts have expired or are no longer associated with a user.

The contractor and subcontractor shall disable accounts for High-Risk Individuals who pose a significant security and/or privacy risk including individuals for whom evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm to the organization and IRS SBU data. Accounts of users identified as posing a high-risk shall have their accounts disabled within one day of discovery of the risk.

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

Call recording systems shall restrict access to only staff initiating or receiving calls.

Call recordings shall not be available for those not participating in the conversation except staff members performing a management designated quality assurance function.

Contractors using a Cloud Service Provider (CSP) shall ensure that they, or the CSP will review privileged access accounts semi-annually and automatically disable inactive accounts after 90 days.

11.3 AC-3 Access Enforcement

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

Role-Based Access Control (RBAC) shall be implemented.

11.4 AC-4 Information Flow Enforcement

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

A few examples of flow control restrictions include: keeping export-controlled information from being transmitted in the clear to the internet; blocking outside traffic that claims to be from within the organization; restricting web requests to the internet that are not from the web proxy server; and limiting information transfers between organizations based on data structures and content.

11.5 AC-5 Separation of Duties

The contractor and subcontractor shall establish appropriate division of responsibilities and separation of duties as needed to prevent harmful activity without collusion.

Duties and responsibilities of functions shall be divided and separated among different individuals, so that no individual shall have all necessary authority and system access to disrupt or corrupt a security process.

11.6 AC-6 Least Privilege

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

The contractor and subcontractor shall authorize access to security functions. Security functions include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, running, and reviewing security scans and establishing intrusion detection parameters.

The contractor and subcontractor shall require that users of system accounts (or roles) with access to security functions or security-relevant information use non-privileged accounts or roles, when accessing non-security functions.

The contractor and subcontractor shall prohibit non-privileged users from executing privileged functions. Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities.

The contractor and subcontractor shall restrict privileged accounts on IT assets, applications, and databases to only those personnel who require access to perform job functions. 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.

All actions performed on the system using privileged roles shall be audited to deter, detect, and report on potential misuse. The contractor shall log the execution of all privileged functions to assist in mitigating the actions of an insider threat or for detection of compromised privileged accounts.

Accounts with administrative privileges (including local administrator rights) shall be prohibited from web browsing, internet connections and accessing email. This can be implemented by establishing separate accounts for privileged users. One account with administrative rights for privileged duties and a standard user account without administrative rights for routine business functions.

Additionally, all returns and return information and other SBU data 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.

In situations where data entry work is being performed, which can include 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; and
- Access to saving files to either an electronic, optical, or other removable media including floppy devices or Universal Serial Bus (USB) devices.

11.7 AC-7 Unsuccessful Login Attempts

All IT assets must be configured to enforce a limit of three 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 a SA or authorized person (or password reset program).

Contractors using a CSP shall ensure that, upon a third unsuccessful logon attempt, they, or the CSP will lock the account for a minimum of 30 minutes and delay the next logon prompt, at a minimum of five seconds.

11.8 AC-8 System Use Notification

Contractor and subcontractor information systems-shall display an interactive information system usage notification (or warning banner) before granting information system access that provides a privacy and security notice.

The warning banner shall state:

- Information system usage shall be monitored, recorded, and subject to audit;
- Unauthorized use of the information system is prohibited and subject to disciplinary actions; and
- The use of the information system indicates consent to monitoring and recording.

For publicly accessible applications or web hosting environments requiring user registration, the application or hosting environment shall:

- Display the information system use information when appropriate, before granting further access;
- 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
- Include in the notice given to public users of the information system, a description of the authorized uses of the system.

The system use notification shall be reviewed and approved by the contractor's legal counsel or an individual designated by the organization's corporate executive.

11.9 AC-11 Device Lock

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

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 and subcontractor information system shall automatically terminate a user session (e.g., application session) after 30 minutes of inactivity.

Session termination addresses the termination of a user session (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions (i.e., network disconnect)). A logical session (for local, network, and remote access) is initiated

whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions.

11.11 AC-14 Permitted Actions without Identification or Authentication

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

The contractor shall employ automated mechanisms to monitor and control remote access methods. Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, laptop computers, workstations, smartphones, and tablets.

Anytime a contractor or subcontractor 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. 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.

- All remote access to the IT environment shall be monitored and controlled.

The information system shall route all remote access through a limited number of managed access control points.

Contractors using a CSP shall ensure that the CSP provides the capability to expeditiously disconnect or disable remote access to the information system within 15 minutes.

11.13 AC-18 Wireless Access

The contractor and subcontractor 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.

Wireless technologies include, but are not limited to, microwave, satellite, packet radio (Ultra-high Frequency (UHF) or Very-high Frequency (VHF), 802.11(x), and Bluetooth.

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.

The contractor and subcontractor shall disable, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.

Only users identified and explicitly authorized shall be allowed to independently configure wireless networking capabilities.

Unapproved wireless networking capabilities of desktops, laptops, printers, copiers, fax machines, and other devices shall be disabled through automated means (where technically possible) and monitored through automated means for unauthorized changes.

One alternative yet acceptable approach to "monitoring through automated means" is regularly pushing out settings that restrict unapproved wireless connections.

Contractors using a CSP shall protect wireless access to the system using authentication of users, devices, and 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.

Contractors and subcontractors shall develop policies for any allowed portable and mobile devices, for information systems that contain SBU data. This includes the use of smartphones, tablets, etc. The policies shall document the approved or disapproved use of mobile devices to connect to IT assets hosting IRS SBU data.

A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source.

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

Laptops and other devices containing IRS SBU data shall not be taken outside of the United States or its territories.

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 Section 21 Physical and Environmental Protection.

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

All mobile computing devices shall employ full-disk encryption. This includes, but is not limited to: IT resources, including computers, laptop computers, Compact Disk (CD), Digital Video Device (DVD) media, thumb drives, or any media that can be used to house IRS SBU 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.

The following controls apply to companies supporting or allowing personally owned devices, also known as Bring Your Own Device (BYOD) that are used to store, process, or access IRS SBU data.

The following features shall be implemented when IRS projects are supported with BYOD platforms:

- All BYOD devices must be registered with the company and controlled via a Mobile Device Manager (MDM) dedicated server;
- Consent to remote inspection and monitoring of the approved mobile access solution on their approved personally owned mobile device;
- Ensure they are the only person who has access to their approved personally owned mobile devices when being used to view or process IRS information;
- Ensure a valid password is successfully entered prior to logging onto the mobile device;
- Only approved personally owned mobile devices shall be permitted to process or store IRS sensitive information, including IRS email;
- The device must have sandboxing capability to segment company and/or IRS data from the employees' personal information. A sandbox is when the MDM installs a password-encrypted environment on the users' mobile devices. These isolated virtual workspaces allow users to manage corporate data and run business apps including their corporate email and meeting software, without having them intermingle with personal data;
- The MDM must have the ability to remotely erase the sand box when the BYOD device is lost, stolen or the employee is no longer working for the company;
- The Sandbox partition must be encrypted utilizing FIPS 140-2 or later, approved encryption;
- Employee-owned applications must not have access to the sandbox;
- All applications stored on the corporate sandbox partition must be approved and distributed by the company via the MDM;

- Employees' personal apps shall not be able to communicate with containerized apps, nor can data be copied and pasted from a containerized app to a non-containerized application;
- BYOD users should not use administrative accounts for general tasks, such as reading email, web browsing, and social networking, because such tasks are common ways of infecting devices with malware;
- The device must include antivirus and anti-malware software with the capability to receive updates automatically. The software shall be configured to scan in real-time and perform full system scans at least weekly;
- The transfer of files via instant messaging platforms shall be restricted. If the software can transfer files with other instant messaging users, it should be configured to prompt the user before permitting a file transfer to begin. File transfers are a common way to transfer malware to other and infect them;
- Jailbreaking or installing a rootkit on BYOD devices is strictly prohibited. Doing so disables the manufacturer's built-in security capabilities for the device. Jailbreaking, in a mobile device context, is the use of an exploit to remove manufacturer or carrier restrictions from a device. The exploit usually involves running a privilege escalation attack on a user's device to replace the manufacturer's factory-installed operating system with a custom kernel;
- The use of public WIFI hotspots is prohibited unless the device is connected via a FIPS 140-2 or later, approved VPN connection;
- A personal firewall must be installed and active on devices that support it;
- Sensitive information (e.g., SBU and PII) shall not be downloaded to mobile devices;
- BYOD participants shall not store any IRS data on a removable memory card;
- IRS SBU shall not be viewed or discussed on mobile devices in public places (e.g., airports, coffee shops, hospitals, malls, etc.); and
- MDM servers shall be configured to detect rooted or jailbroken devices.

Contractors using a CSP shall ensure that the CSP employs either full-device encryption or container encryption to protect the confidentiality and integrity of information on any type of mobile device.

11.15 AC-20 Use of External Systems

External systems are information systems or components of said 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 and subcontractor 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 and subcontractor 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.

The contractor and subcontractor 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:

- Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; and
- 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 and subcontractor 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.

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

This requirement applies to information that may be restricted in some manner (e.g., contract-sensitive information, proprietary information, PII, SBU data based on some formal or administrative determination). Depending on the 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 and subcontractor 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:

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

12.0 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 Awareness and Training Policy and Procedure

The contractor and subcontractor shall designate an official to manage the development, documentation, and dissemination of the AT policies and procedures. The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

Contractors and subcontractors shall review/update those policies and procedures every three years, 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 AT. This also applies to contractors and subcontractors working at contractor-managed facilities using contractor-managed IT assets. The IRS will provide the required training to contractors.

12.2 AT 2 Literacy Training and Awareness

The IRS Security Awareness Training is a combination of the mandatory briefings that cover: Cybersecurity Awareness/Information System Security, Privacy Information Protection and Disclosure, Unauthorized Access to Taxpayer Data, Records Management, Inadvertent Sensitive Information Access, and/or Facilities Physical Security.

For each contractor and subcontractor employee assigned to a contract/order that is not connected to the IRS infrastructure, the contractor shall submit confirmation of completed Security Awareness Training to the COR.

Contractors and subcontractors who have access to the IRS infrastructure must complete Security Awareness Training via the IRS online training system.

IRS Security Awareness Training must be completed by contractor/subcontractor personnel within five business days of successful resolution of the suitability and eligibility for staff-like

access as outlined in IR1052.224-9001 Mandatory IRS Security Training for Information Systems, Information Protection and Facilities Physical Access and before being granted access to SBU data. Thereafter, each contractor and subcontractor employees assigned to the contract/order shall complete IRS Security Awareness Training annually by October 31. The date listed on the memorandum provided by IRS Personnel Security shall be used as the commencement date.

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.

12.3 AT-3 Role Based Training

Any contractor employee who has a significant IT security role or responsibility shall complete specialized IT security (SITS) training pertinent to the role/responsibility. This includes, but is not limited to, any contractor or subcontractor employees 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 the COR.

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 five business days of being granted staff-like access approval by Personnel Security. Thereafter, each contractor and subcontractor employee assigned to the contract/order shall complete Awareness Training annually by June 1 of each calendar year.

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 SITS Training within 45 days of the contract modification designating an employee to a specialized IT security role and annually, by June 1, thereafter.

12.4 AT-4 Training Records

The contractor shall provide all security and privacy training records to the COR for training completed outside of the IRS learning system. The COR is responsible for uploading the training completions into the IRS learning system. The IRS learning system retains the training records.

13 Audit and Accountability (AU)

For all contractors and subcontractors, where more than one 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 and Accountability Policy and Procedures

Contractors and subcontractors shall designate an official to manage the development, documentation, and dissemination of the AU policies and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

Contractors and subcontractors shall review/update those policies and procedures every three years, or if there is a 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 Event Logging

At contractor sites, event logging shall be implemented to record and monitor access to IT assets, including, but not limited to routers, operating systems, databases, remote access, and applications. Audit records shall be sufficient to enable re-creation of information system related events.

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

Table 2: Logging Events

1	Log onto system
2	Log off system

3	Change of Password
4	All System Administrator (SA) commands, while logged on as a SA
5	Clearing of the audit log file
6	Startup and shut down of audit functions
7	Use of identification and authentication mechanisms (e.g., user id and password)

Contractors and subcontractors using application systems including Commercial Off-the-Shelf (COTS) solutions to store, process, and collect FTI must retain event logs to support audit analysis and investigations of unauthorized access. The system must record and retain the following information in a data transaction or event log; the user identity, date and time of access to FTI, action taken, and which account was accessed.

Call recording application systems must have the ability to capture and retain call recording meta-data. Meta-data associated with the voice recording must include the following:

- The staff member initiating or receiving the call;
- The data, time and duration of the conversation;
- A means to track the identity of the customer; and
- Any subsequent access to the voice recording (to identify UNAX violations).

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; and
- The identity of any individuals, subjects, or objects/entities associated with the event.

13.4 AU-4 Audit Log Storage Capacity

Audit log storage capacity shall be allocated to accommodate audit log retention requirements. Audit log retention shall be sufficient to enable log management and retrieval of auditable events as necessary. Log storage capacity shall be defined in the system security documentation.

13.5 AU-5 Response to Audit Logging 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 and subcontractor shall develop and implement an action plan that can be used in an audit processing failure.

Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Real-time message alert mechanisms shall be implemented at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

13.6 AU-6 Audit Record Review, Analysis, and Reporting

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

The contractor and subcontractor shall employ automated mechanisms to integrate audit review, analysis, and reporting processes to support contractor processes for investigation and response to suspicious activities.

A call recording application system must have the ability to search the meta-data for the purposes of play-back, quality assurance, and a record of file access.

Automated audit reports/records shall be generated, analyzed, and correlated across different repositories to gain contractor-wide situational awareness.

Integrated analysis requires that the information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information.

Audit record review, analysis, and reporting covers information security- and privacy-related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP).

For any compromise to IRS SBU data, this shall be identified as an information security incident, and reported to the IRS CSIRC Incident Response Operations Team at (240) 613-3606**.** See procedures in Incident Response and Incident Reporting section of this document.

Contractors using a CSP shall ensure that they, or the CSP will review and analyze information system audit records at least weekly; for indications of inappropriate or unusual activity.

13.7 AU-7 Audit Record Reduction and Report Generation

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

The information system shall provide the capability to automatically process audit records (sort and search) 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 the Coordinated Universal Time (UTC), Greenwich Mean Time (GMT), or Local Time with an offset from UTC.

Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within hundreds of milliseconds or tens of milliseconds).

The contractor and subcontractor shall compare internal information system clocks with an authorized enterprise-wide time source and synchronize the internal system clocks to the authoritative time source when the time difference is greater than one minute.

13.9 AU-9 Protection of Audit Information

The contractor and subcontractor shall identify all individuals who are responsible for reviewing audit information upon detection of unauthorized access, modification, or deletion. 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 data. 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 the SA. A privileged group shall be established to access audit information and support systems. It is best practice to have separate privileges established for audit and SA functions.

Contractors using a CSP shall ensure that they or the CSP will back up audit records at least weekly onto a physically different system, or system component than the system or component being audited.

13.10 AU-11 Audit Record Retention

Audit records must be retained for a period of seven years if there are returns or return information. Otherwise, they shall be retained for three years for the purpose of providing support in after-the-fact investigations of security incidents. Copies shall be provided to the IRS when requested to investigate potential IRS impacted events.

Contractors using a CSP shall ensure that they or the CSP shall ensure that the audit records are retained online for a minimum of 90 days for the following time periods to provide support for after-the-fact investigations of security incidents

Off-line storage to support this requirement must be tested to ensure that the data can be recovered and available for analysis.

13.11 AU-12 Audit Record 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 audit all accesses to that directory.

The information system shall have the capability to allow the selection of auditable events for specific information system components.

14.0 Assessment, Authorization, and Monitoring (CA)

An assessment of the controls provides the contractor and IRS with an assurance that security and privacy 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 and privacy 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 and privacy 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 Assessment, Authorization, and Monitoring Policies and Procedures

The contractor and subcontractor shall designate an official to manage the development, documentation, and dissemination of the security assessment and authorization policies and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

The contractor shall review/update the policies and procedures every three years, immediately after a security breach, or if there is a significant change. Events that may precipitate an update to assessment, authorization, and monitoring policy and procedures include security assessments, audit findings, and security or privacy incidents.

14.2 CA-2 Control Assessments

The contractor shall develop a security and privacy control assessment plan and produce a Control Assessment Report (CAR) with the results of the assessment. The contractor shall

ensure the security and privacy control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment.

The assessment shall be conducted annually or when major changes have been made to the IT environment to ensure the security and privacy controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the IT environment.

When testing of a security or privacy control reveals that the control is not functioning as expected and corrective action has been taken to mitigate the weakness, the finding and corrective action shall be documented within the testing documentation.

The results of security and privacy control assessments shall be documented in a CAR.

14.3 CA-3 Information Exchange

The contractor shall maintain an authorization list that defines the external systems.

System to system connections is to be authorized and documented via an Interconnection Security Agreement (ISA). The ISA shall be reviewed and updated (if necessary) at least annually.

For each system interconnection the contractor/subcontractor shall document the interface characteristics, security and privacy requirements, controls, and responsibilities for each system.

The contractor, based on a risk assessment, shall employ the policy for allowing contractor IT assets to connect to external information systems:

- Deny-all, permit-by-exception.

The contractor and subcontractor shall configure all equipment connected to the contractor system or network where IRS data is being processed or stored, to meet Publication 4812 requirements.

This control applies to dedicated connections between the information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing or to connections with external providers who are only providing telecommunications and transmission services.

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. The contractor and

subcontractor shall update an existing POA&M on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

POA&M updates shall be provided by the contractor to the COR or delegate at a minimum quarterly, demonstrating progress made toward weakness remediation.

14.5 CA-6 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 authorization is reviewed and updated every 3 years, or when a significant impact to the information system occurs.

At a minimum, the final Authorization package(s) shall consist of the following deliverables:

- System Security Plan (SSP);
- Security Assessment Report (SAR);
- Any active POA&M;
- Any Memorandum of Understanding (MOU);
- Auditing plan; and
- Security Authorization Decision Document.

The System Security Plan (SSP) shall contain the following either internally or as supporting appendices.

- Security Risk Assessment (SRA)
- Any Interconnection Agreement
- Information System Contingency Plan
- Security Configuration Documentation
- Configuration Management Plan
- Incident Response Plan
- Continuous Monitoring Plan
- Implemented Security Controls

14.6 CA-7 Continuous Monitoring

All contractors and subcontractors 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.

The contractor and subcontractor shall implement a continuous monitoring strategy that includes active and ongoing monitoring of the security controls (e.g., monthly policy checking

and vulnerability scans) and privacy controls, in accordance with the defined configurations to identify any controls that may not be compliant. The contractor and subcontractor shall report the security and privacy status of the system to the Contractor Security Representative (CSR).

The contractor and subcontractor shall ensure risk monitoring is an integral part of the continuous monitoring strategy, including;

- Effectiveness monitoring,
- Compliance monitoring, and
- Change monitoring

Contractors using a CSP shall ensure that the CSP conducts operating system (OS) scans and web application scans at least monthly. All scans shall be performed annually by an independent assessor.

14.7 CA-8 Penetration Testing

The contractor and subcontractor shall conduct penetration testing on information systems at a minimum every three years using risk assessments to establish testing prioritization.

Contractors using a CSP shall ensure that the CSP will conduct penetration testing at least annually on all information systems or system components. An independent penetration agent or team shall be employed.

14.8 CA-9 Internal System Connections

The contractor shall authorize any internal connections to IT assets processing IRS SBU data and document the interconnection characteristics, security and privacy requirements, and the type of information being transmitted between IRS assets and any other internal contractor information systems. The contractor shall review connections annually to ensure connections are still needed.

15.0 Configuration Management (CM)

CM 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 and subcontractor shall designate an official to manage the development, documentation, and dissemination of the CM policy and procedures. Security and privacy programs shall collaborate on the development of the CM policy and procedures

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

The contractor and subcontractor shall review/update CM policies and procedures every three years, 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 and subcontractor 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.

- The contractor and subcontractor shall review and update the baseline configuration of the information system:
  - Annually,
  - When required due to a significant change, and
  - As an integral part of information system component installations and upgrades.
- The contractor and subcontractor shall retain older versions of baseline configurations as deemed necessary to support rollback.
- The contractor and subcontractor shall use automated mechanisms to retain the current configuration baselines. Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools.

- The contractor and subcontractor shall maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.

The contractor and subcontractor 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 controls (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 and subcontractor shall develop and implement a change control process. This process shall include a formal written change request to be submitted to the appropriate Change Control Board (CCB) for all changes, scheduled and unscheduled. The CCB shall include information security and privacy representatives. This process shall ensure that all changes are approved, tested, documented, and published; using a change control log and is available for review. This log shall be retained using automated tools, such as: electronic spreadsheets, databases, etc.

Development and testing environments shall be physically and/or logically separated from production environments.

Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, vulnerability remediation and unscheduled or unauthorized changes. For changes that impact privacy risk, the CSR for privacy shall update privacy impact assessments.

Change logs will be retained for three years as confirmed by the IRS Records and Information Management (RIM) Office. 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 Impact Analysis

Changes to information systems shall be analyzed in a test environment prior to implementation into the production environment as part of the change approval process to determine potential security and privacy impacts.

Impact analysis may include, for example, reviewing security and privacy plans to understand control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security and privacy impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security or privacy controls are required.

15.5 CM-5 Access Restrictions for Change

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

The contractor and subcontractor shall limit privileges to change information system components and system-related information within a production or operational environment; and review and reevaluate privileges at least quarterly.

The contractor and subcontractor shall take measures to protect devices against the bypass of software controls arising from booting from any sources other than those designated by the SA for such purposes.

15.6 CM-6 Configuration Settings

The contractor and subcontractor shall establish and document configuration settings for information technology products employed within the information system using security configuration tools. Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system.

The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluations. The specifications comprising SCAP include Extensible Markup Language (XML) and enumerations. Working in conjunction, vulnerability and compliance information can be shared and executed between any SCAP enabled products. Vulnerability and policy content created using SCAP can be used with any SCAP-validated product to perform vulnerability management, measurement, and policy compliance evaluations.

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

The contractor and subcontractor shall use SCAP approved tools when monitoring security configurations. A list of SCAP approved products can be found at https://csrc.nist.gov/Projects/scap-validation-program/validated-products-and-modules.

Contractors using a CSP shall ensure that they or the CSP verify that the configuration settings are established and documented for information technology products employed within the information system using United States Government Configuration Baseline (USGCB).

I. If USGCB is not available, the service provider shall use the Center for Internet Security (CIS) guidelines (Level 1) to establish configuration settings.

II. The service provider shall ensure that checklists for configuration settings are SCAP validated.

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, software, and services. Employees performing data entry do not require SA or elevated privileges.

Protocols, services, and logical ports that shall be restricted, including 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 and during transition periods from older technologies to newer technologies, 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 and subcontractor shall identify all programs authorized to be used and not allowed in the IT environment and defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions.

- The contractor and subcontractor shall review the information system at least annually and during transition periods from older technologies to newer technologies to identify and disable unnecessary functions, ports, protocols, software and/or services.
- The information system shall prevent unauthorized software from being executed.
- The contractor and subcontractor shall identify all programs authorized to be used on the information system. A “deny-all, allow-by-exception” policy shall be employed to prohibit the execution of unauthorized programs. The list of authorized programs shall be reviewed and updated at a minimum annually. By default, the contractor shall maintain the most restrictive permissions and use of programs.

The contractor and subcontractor shall scan their networks, at minimum, annually to detect and remove any unauthorized or unlicensed software.

Contractors using a CSP shall ensure that they or the CSP configure the information system to provide only essential capabilities. The service provider shall use the CIS guidelines to establish a list of prohibited or restricted functions, ports, protocols, and/or services; or establish its own list of prohibited or restricted functions, ports, protocols. The information system shall prevent program execution using a list of authorized software programs (i.e., whitelist. Review and update the list of authorized software programs at least annually.

15.8 CM-8 System Component Inventory

The contractor and subcontractor shall develop, document, and maintain an inventory of all hardware, software, and removable media that accurately reflects the current information and includes all components of the information system to support IRS work. The inventory shall include: an inventory serial number, description of the inventory item, owner of the inventory item, date placed in inventory, and date inventory was validated. The inventory shall not include duplicate accounting of components or components assigned to any other system. 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.

- The contractor and subcontractor shall update the inventory of information system components as an integral part of component installations, removals, and information system updates.

The contractor and subcontractor shall:

- Employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
- Take the following action when unauthorized components are detected:
    - Disable network access by such components,
    - Isolate the components, and
    - Notify appropriate officials.

Contractors using a CSP shall ensure that they or the CSP employ automated mechanisms continuously, with a maximum five-minute delay in detection to detect the presence of unauthorized hardware, software, and firmware components. Upon detection, network access shall be disabled.

15.9 CM-9 Configuration Management Plan

The contractor and subcontractor shall develop, document, and implement a CM plan for the information system that addresses roles, responsibilities, and CM processes and procedures. A process shall be established for identifying configuration items throughout the System Development Life Cycle (SDLC) 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 CM. The CM plan shall be reviewed and approved by contractor-defined personnel and protected from unauthorized disclosure and modification.

15.10 CM-10 Software Usage Restrictions

The contractor and subcontractor shall use software and associated documentation in accordance with contract/order/agreement and copyright laws. The contractor and subcontractor shall track the use of software quantity licenses. The contractor and subcontractor shall 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 software.

15.11 CM-11 User-Installed Software

The contractor and subcontractor 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 and subcontractor shall develop and manage a process to apply all software changes to the environment.

Permitted software installations include downloading new applications from organization-approved "app stores." Prohibited software installations include software with unknown or suspect pedigrees, or software that organizations consider potentially malicious.

15.12 CM-12 Information Location

The contractor and subcontractor shall identify and document:

- The location of IRS SBU data and the specific system components on which the information is processed and stored, and
- The users who have access to the system and system components where the information is processed and stored.

The contractor and subcontractor shall utilize automated information location tools to manage the data produced during information location activities and share information across the organization. Changes to the location where the information is processed and stored shall be tracked and documented.

16.0 Contingency Planning (CP)

All contractors and subcontractors 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 and subcontractors shall designate an official to manage the development, documentation, and dissemination of the CP Policy and Procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

The contractor and subcontractor shall review/update CP policies and procedures annually, or if there is a significant change that defines company requirements in terms of IT CP, or following certain events including: assessment or audit findings, and security or privacy incidents.

The contingency plan shall be updated to address changes to the organization, system, or environment of operation, and problems encountered during contingency plan implementation, execution, or testing. Lessons learned from contingency plan testing, training, or actual contingency activities shall be incorporated into contingency testing and training.

The policies and procedures shall be sufficient to address the planning elements required for a contractor or subcontractor site. Policies and procedures shall address the need to identify essential business functions supported, provide restoration priorities, and identify contingency roles and responsibilities.

Disaster recovery plans shall be developed, tested, and maintained for mission or business critical systems for use in the event that normal operations cease.

16.2 CP-2 Contingency Plan

All contractors and subcontractors shall develop contingency plans to address IT and physical security planning. Contingency plans 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 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, updated, and the contractor shall conduct OEP drills, documenting the results, and incorporating lessons learned into the OEP.

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

The contingency plan is considered SBU data and shall be protected from unauthorized disclosure and modification.

The contractor and subcontractor shall coordinate contingency plan development with contractor groups responsible for related plans. Related plans include: Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and OEP.

The contractor and subcontractor shall plan for the resumption of essential missions and business functions within a specified period of time upon contingency plan activation.

The contractor and subcontractor shall identify critical information system assets supporting essential mission and business functions.

16.3 CP-3 Contingency Training

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

Training content shall be updated annually, when there are major system changes, or following certain events including: contingency plan testing, security or privacy assessments, audit findings, and security or privacy incidents.

16.4 CP-4 Contingency Plan Testing

All contingency plans shall be tested at least annually. The contractor and subcontractor shall develop and test a plan to ensure that operations can be restored. The contractor and subcontractor 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.

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

Contractors using a CSP shall require the CSP to test the contingency plan for an information system to determine the effectiveness of the plan and the organizational readiness to execute the plan at a minimum annually using functional exercises.

16.5 CP-6 Alternate Storage Site

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

Potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster shall be identified and explicit mitigation actions outlined.

Contractors using a CSP shall require the CSP to establish an alternate storage site including necessary agreements to permit the storage and retrieval of backup information; and ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

16.6 CP-7 Alternate Processing Site

The contractor and subcontractor shall establish an alternate processing site, including the necessary agreements to permit the transfer and resumption of information systems operations for essential mission and business functions within specified timeframes consistent with the RTO and RPO.

The contractor and subcontractor 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. Alternate processing sites are locations that are sufficiently separated from the primary processing sites to reduce susceptibility to the same threats. The systems, personnel, and physical security controls shall be commensurate with the sensitivity of the information being restored, and with the security of the primary processing site.

Potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster shall be identified and explicit mitigation actions shall be outlined.

Alternate processing site agreements shall be developed that contain priority-of-service provisions (e.g., Service Level Agreements (SLA)) in accordance with the organization's availability requirements (including the RTO).

Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements, and the availability of information resources at the alternate processing site.

Contractors using a CSP shall ensure that the CSP has established an alternate processing site, including the necessary agreements to permit the transfer and resumption of information system operations. An alternate processing site shall be identified that is separated geographically from the primary processing site to reduce susceptibility to the same threats.

16.7 CP-8 Telecommunications Services

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

The contractor and subcontractor shall develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the contractor's availability requirements.

The contractor and subcontractor shall obtain alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

Contractors using a CSP shall ensure that the CSP has established alternate telecommunications services, including the necessary agreements to permit the transfer and resumption of information system operations.

16.8 CP-9 System Backup

The contractor and subcontractor shall backup information system documentation weekly, including security-related documentation. Backups include user-level information, system-level information, including security and privacy related documentation, and SBU data. The contractor and subcontractor shall test backup information semi-annually to verify media reliability and information integrity.

System-level information includes, for example, system-state information, OS and application software, and licenses. User-level information includes any information other than system level information.

The contractor and subcontractor shall protect the confidentiality, integrity, and availability of backup information at storage locations.

The contractor and subcontractor shall implement FIPS 140-2, or later compliant cryptographic mechanisms to prevent unauthorized disclosure and modification of backup information.

Contractors using a CSP shall ensure that they or the CSP will conduct backups for information contained in the information system at the following frequencies:

- User-level: daily incremental, weekly full;
- System-level: daily incremental, weekly full; and
- Information system configuration: daily incremental, weekly full.

The contractor or CSP shall maintain:

- At least three backup copies of user-level information (at least one of which is available online) or provide an equivalent alternative;
- At least three backup copies of system-level information (at least one of which is available online) or provide an equivalent alternative;
- At least three backup copies of information system documentation including security information (at least one of which is available online) or provide an equivalent alternative; and
- Backup information shall be tested to verify media reliability and information integrity at least annually.

16.9 CP-10 System Recovery and Reconstitution

The contractor and subcontractor shall ensure that 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 within a timeframe consistent within the contractor defined RTO and RPO.

Transaction recovery for information systems that are transaction based shall be implemented.

Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.

Contractors using a CSP shall ensure that the CSP shall provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure

17.0 Identification and Authentication (IA)

IA are the stages of one process that is used to identify an individual (e.g., username) 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 and subcontractor shall designate an official to manage the development, documentation, and dissemination of the IA policies and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

Policies and procedures shall be reviewed/updated every three years, or if there is a significant change to facilitate implementing IA 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 IA to access this asset. Typically, this is known as a username 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 and subcontractor shall ensure that information systems uniquely identify and authenticate all devices before allowing a connection to the contractor's network.

Organizational devices requiring unique device-to-device IA may be defined by type, device, or a combination of type/device. Information systems typically use one of the following to identify and authenticate devices on local and/or wide area networks:

- Shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) for device identification; or

- An organizational authentication solution (e.g., Institute of Electrical and Electronics Engineering (IEEE) 802.1(x) and Extensible Authentication Protocol (EAP), Radius server with EAP-TLS authentication, Kerberos).

17.4 IA-4 Identifier Management

The contractor and subcontractor shall manage all identifiers (e.g., usernames) for either systems or IT assets to include the following:

- All default vendor or factory-set administrative accounts and passwords shall be changed prior to implementation (i.e., during installation or immediately after installation).
- Establishing user accounts, only after receiving authorization from an individual assigned and authorized to approve new user accounts, user roles, groups, etc.
- Manage individual identifiers by uniquely identifying each individual with their status. Status identifiers include contractors, subcontractors, etc. Identifying the status of individuals by these characteristics provides additional information about the people with whom contractor personnel are communicating.
- 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
- Ensuring that usernames or similar accounts cannot be reused.

17.5 IA-5 Authenticator Management

Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). The contractor and subcontractor information system for password-based authentication shall implement the following password settings:

- Passwords for windows-based systems must contain a minimum of 12 characters for user accounts.
- Passwords for all other systems must contain a minimum eight characters.
- Passwords for service accounts must contain a minimum of 14 characters.
- Enforce password complexity, to contain a combination of letters, numbers, and special characters for all information system accounts.
- For windows-based systems; enforce a password minimum lifetime restriction of one day and maximum of 60 days.
- For all other systems; enforce a password minimum lifetime restriction of one day and maximum of 90 days.
- Prohibit password reuse for 24 generations for workstations/laptops, and 10 generations for all other systems.
- Encrypt passwords in storage and transmission.

- New passwords selected for use shall have at least one character changed from the previous password.
- Allow the use of a temporary password for system logons, with an immediate change to a permanent password.

When Public Key Infrastructure (PKI) is used in the information system it shall:

- Validate certificates by constructing a certification path with status information to an accepted trust anchor, including checking certificate status information.
- Implement a local cache of revocation data to support path discovery and validation.
- Enforce authorized access to the corresponding private key.

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.

The contractor and subcontractor shall require that the registration process to receive Homeland Security Presidential Directive-12 (HSPD-12) PIV card be carried out in person, with a designated registration authority with authorization, by a designated contractor official (e.g., a supervisor). This only applies when contractors or subcontractors are also accessing IRS systems and/or facilities.

The contractor and subcontractor 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.

For IT devices using a personal identification number (PIN) as an authenticator, the PIN shall meet the following requirements:

- Eight digits minimum length; If unable to meet the minimum length, then the maximum length possible shall be used;
- Be complex (e.g., 73961548);
- No repeating digits (e.g., 44444444 or 12121212);
- No sequential digits (e.g., 12345678, 87654321); and
- Not be shared.

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 during implementation.

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

Users shall protect passwords, hardware tokens, and/or smart cards, and ensure they are not stored on, or with a laptop or portable electronic device (PED), unless encrypted or otherwise under the direct and continuous control of the authorized user.

Contractors using a CSP shall ensure that they or the CSP will manage information system authenticators by changing/refreshing authenticators, including passwords, every 60 days.

Passwords shall be:

- Complex with a minimum of 12 characters; case sensitive, and at least one each of upper-case letters, lower-case letters, numbers, and special characters;
- Password enforcement shall provide lifetime restrictions of one day minimum and sixty days maximum; and
- Passwords shall be prohibited from reuse for 24 generations.

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 unauthorized individuals.

Desktop and laptop assets have relatively large monitors, and the threat of shoulder surfing can be significant.

17.7 IA-7 Cryptographic Module Authentication

When contractors and subcontractors 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 and subcontractors 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-Organizational Users)

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

18.0 Incident Response (IR)

A security incident as defined by OMB 17-12 is an occurrence that:

- Actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
- Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

A data breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

- a person other than an authorized user accesses or potentially accesses PII; or
- an authorized user accesses or potentially accesses PII for other than authorized purpose.

A data breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment (See Table 3 for examples of Security Incidents and Data Breaches).

Often, an occurrence may first be identified as an incident, but later identified as a data breach once it is determined that the incident involves PII, as is often the case with a lost or stolen laptop or electronic storage device. For the purposes of this section when referring to "incidents" it will include data breaches.

Whenever there is a compromise of IRS information, the contractor and subcontractor shall contact the IRS immediately upon discovery of the incident or potential incident. The IRS shall work closely with IRS contractors and subcontractors to quickly respond to a suspected incident of unauthorized disclosure or inspection.

Types of incidents include the following:

Table 3: Examples of Security and Privacy 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 or more incident types.
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 and subcontractor shall designate an official to manage the development, documentation, and dissemination of the IR policies and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

The contractor and subcontractor shall 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 and subcontractor 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).

IR Training for contractors assuming an incident response role is due within 30 days of assuming an incident response role and responsibility, when required by information system changes, or when acquiring system access, and annually thereafter.

18.3 IR-3 Incident Response Testing

The contractor and subcontractor shall annually test and/or exercise the IR capability to determine the incident response effectiveness and document the results to ensure the policies and procedures continue to function, as intended. Contractors and subcontractors shall review NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide for guidance on developing and maintaining their IR capabilities. Testing results shall be documented, and incident response policies and procedures shall be updated to close any gaps found in the plan.

Incident response testing includes reporting phone numbers identified in contractor procedures are accurate; the use of checklists, walk-through, or tabletop exercises; simulations (parallel/full interrupt); and comprehensive exercises.

Incident response test results, findings, and plan updates shall be shared with the CO and COR upon completion.

Contractors using a CSP shall ensure that the CSP shall test the IR capability for information systems to determine the incident response effectiveness and document the results at least annually.

18.4 IR-4 Incident Handling

Contractors and subcontractors are required to maintain capabilities to determine what IRS SBU data was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access IRS SBU data, and identify the initial attack vector.

The contractor and subcontractor 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 and subcontractors shall routinely track and document security incidents potentially affecting the confidentiality of SBU or PII data. An incident that involves PII is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses, or potentially accesses PII or an authorized user accesses or potentially accesses such information for other than authorized purposes. Where contractors rely on IT technical support, the contractors shall ensure the IT support teams address the need to manage and track incidents.

Automated mechanisms shall be employed to support the incident handling process. This includes online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

18.5 IR-5 Incident Monitoring

The contractor and subcontractor shall track and document all security incidents, data breaches and Privacy related incidents. Contractors and subcontractors shall; maintain records about each incident, the status of the incident, and other pertinent information needed for forensics, evaluating incident details, and trend analysis.

Incident information can be obtained from sources, network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports.

18.6 IR-6 Incident Reporting

Contractors and subcontractors shall report a suspected incident or confirmed breach in any medium or form, including paper, oral, and electronic immediately upon discovery.

Automated mechanisms shall be employed to assist in the reporting of incidents. Automated reporting mechanisms include email, posting on websites (with automatic updates), and automated incident response tools and programs.

Security and Privacy incidents related to IRS processing, SBU data, or contractor information systems shall be reported immediately upon discovery to the CO and COR and the CSIRC Incident Response Operations Team at (240) 613-3606. Within one hour of notification of the incident the COR shall complete the Computer Security Incident Reporting Form available at https://www.csirc.web.irs.gov/reporting/. Physical incidents shall be referred to the Situational Awareness Monitoring Center (SAMC) at (866) 216-4809. In those situations where there is a physical security incident involving IRS processing, SBU date or contractor information systems, both CISRC and SAMC shall be contacted. CSIRC is available 24x7x365.

If the incident/data breach involves returns or return information or threatens the safety or security of personnel or information systems, or involves a ***willful***, unauthorized disclosure, the COR shall also report the incident/data breach to the Treasury Inspector General for Tax Administration (TIGTA) hotline at (800) 366-4484.

Failure of the contractor and subcontractor to notify the IRS in the event of an incident within the required timeframe shall be considered a breach of contract. The IRS reserves the right to remedies such as termination of the contract or assess liquidated damages as allowed with FAR clause 52.211-11 -- Liquidated Damages -- Supplies, Services, or Research and Development (September 2000).

18.7 IR-7 Incident Response Assistance

All contractors and subcontractors shall identify IR resources (help desk or incident response team) who shall provide assistance with the handling of potential incidents. The support resources shall have adequate training and understanding to help resume business operations, while providing support to contain and manage a potential incident.

Automated mechanisms shall be employed to increase the availability of IR related information and support.

Based on the severity and potential impact of an incident, the IRS reserves the right to provide IR assistance. IRS assistance can include; inspection, investigation, forensic analysis, and recovery operations. The contractor and subcontractor shall provide support and fully cooperate with IRS staff should their services be warranted.

18.8 IR-8 Incident Response Plan

The contractor and subcontractor shall develop and annually review an IR plan that provides a high-level approach to handle incidents. The plan shall:

- Provide the organization with a roadmap for implementing its IR capability;
- Describe the structure and organization of the IR capability;
- Provide a high-level approach for how the IR capability fits into the overall organization;
- Meet the unique requirements of the organization, which relate to mission, size, structure, and functions;
- Define reportable incidents;
- Address the sharing of incident information;
- Explicitly designate responsibility for IR to personnel/team;
- Update the IR plan to address system and organizational changes, or problems encountered during plan implementation, execution, or testing;
- Provide metrics for measuring the IR capability within the organization;
- Define the resources and management support needed to effectively maintain and mature an IR capability;
- Be reviewed and approved by CSR; and
- Protect the IR plan from unauthorized disclosure and modification.

All access to call recording data shall be tracked in the application system, to support UNAX investigations.

19.0 Maintenance (MA)

Maintenance ensures that all IT assets are available and ensures the integrity and reliability of the equipment. All contractors and subcontractors shall rely on the operation and functionality of equipment if they are to provide continued service to the IRS.

19.1 MA-1 Maintenance Policy and Procedures

The contractor and subcontractor shall designate an official to manage the development, documentation, and dissemination of the maintenance policy and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and

- Compliance.

The contractor and subcontractor shall review/update policies and procedures every three years, 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 and subcontractor shall establish a formal information systems maintenance program, that applies to all types of maintenance to all system components (including but not limited to; applications, servers, workstations, storage arrays, routers, switches, firewalls, scanners, copiers, and printers) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement).

Changes made to hardware or software during maintenance shall be recorded per configuration management processes for the hardware or software.

The contractor and subcontractor 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; and
- Information system components/equipment removed or replaced (including identification numbers, serial numbers, and/or barcodes, if applicable).

The contractor and subcontractor 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 Vendor POC 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 for off-site maintenance, repair, or replacement. 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 verify the controls are still functioning properly.

Contractors using a CSP shall ensure that the CSP schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications. Approve and monitor all maintenance activities, whether performed on-site or remotely and whether the equipment is serviced on-site or

removed to another location. Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.

19.3 MA-3 Maintenance Tools

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

This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on contractor and subcontractor information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally.

Maintenance tools shall be checked for malicious code before installation on information systems. 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.

The contractor and subcontractor shall inspect all the maintenance tools carried into a facility by maintenance personnel for obvious improper or unauthorized modifications. The contractor shall review approved system maintenance tools annually.

Contractors using a CSP shall ensure that the CSP approves, controls, and monitors information system maintenance tools. Maintenance tools carried into a facility by maintenance personnel shall be inspected for improper or unauthorized modifications. Media containing diagnostic and test programs shall be checked for malicious code before the media is 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, VPN, or other communication path to access the contractor's IT assets.

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

- Contractor 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;
- 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 and subcontractor personnel providing internal IT support, non-local maintenance shall be documented and periodically reviewed by the contractor. The contractor shall document in the security plan for the: information system, installation, and the use of non-local maintenance and diagnostic connections.

19.5 MA-5 Maintenance Personnel

The contractor and subcontractor shall establish a process for authorizing maintenance personnel and maintaining a list of authorized maintenance organizations/personnel. Non-escorted personnel performing maintenance on the information system shall have the required access authorizations. The contractor and subcontractor 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 and subcontractor 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.

20.0 Media Protection (MP)

MP 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 IRS SBU data. 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.

NIST defines three classes of sanitization. These are clear, purge, and destroy based on the definitions below:

- **Clear -** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using methods such as Secure Erase.
- **Purge -** applies physical or logical techniques that render target data recovery infeasible using state of the art laboratory techniques.
- **Destroy -** renders target data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

Use of a sanitization class is dependent on the following conditions:

- If the media will not be reused, then it must be destroyed. This would apply to CDs, hardcopy, and decommissioned or inoperable disk drives and storage arrays.
- The media must be purged if it will be reused, but not under the direct physical control of the contractor.
- If the media will be reused and remain under the direct control of the contractor's environment, then the clearing of IRS SBU data is acceptable.

The most common way to clear data is to perform a disk wipe using a software tool that overwrites all sectors of the disk with positive and negative (0 and 1) values. IRS standards require seven overwrites when the data contains FTI, otherwise three passes are acceptable. Full-disk wipes shall be applied to workstations and laptops. Software tools that have been validated by the International Standards Organization (ISO) are:

- Windows - BCWipe Total WipeOut, Darik;s Boot and Nuke (DBAN), and Parted Magic.
- MAC - BCWipe Total WipeOut.
- UNIX/Linux - BCWipe Total WipeOut, Darik;s Boot and Nuke (DBAN), and Parted Magic.

Partial data clearing can be appropriate for IRS data stored on file servers that also contain other customer information. There are a variety of software tools that can be used to overwrite selected files and folders, thus retaining the data of other customers. Software tools that have been validated by the International Standards Organization (ISO) are:

- Windows - BCWipe, Erasure, Identity Finder, and Microsoft SDelete.
- MAC - BCWipe, and Secure Empty Trash.
- UNIX/Linux - BCWipe, and SRM.

Methods of purging data include; overwrite, block erase, and cryptographic erase. Overwrite is the clear method described above but does require a full-disk wipe. Block and cryptographic erase methods are options that are dependent on the device manufacture.

Another purge option is the use of a degausser. A degausser generates a magnetic field that applies a unidirectional alignment to the data recording surface. Degaussing renders many types of devices unusable (and in those cases, degaussing is also a destruction technique).

Destruction methods are designed to physically destroy the data through disintegration, pulverization, melting, or incineration. However, bending, cutting, and the use of some emergency procedures (such as using a power drill or hammer) are not acceptable methods of media destruction as portions of the media may remain undamaged and therefore accessible using advanced laboratory techniques.

Paper shredders can be used to destroy hard copy materials and flexible media such as diskettes once the media are physically removed from their outer containers. In-office shredders must produce crosscut particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller).

Contractors and subcontractors may elect to use an on-site shredding service vendor. Use of these services in lieu of deploying in-office shredders must adhere to the following standards:

- Materials to be shred must be deposited in locked containers with key registration under management control;
- Shredding must be performed on-site under the direct observation of an IRS cleared contractor staff member;
- The shred vendor must hold National Association for Information Destruction (NAID) certification; and
- The shred vendor shall provide the contractor with a certificate of destruction before leaving the facility.

20.1 MP-1 Media Protection Policy and Procedures

The contractor and subcontractor shall designate an official to manage the development, documentation, and dissemination of the MP policies and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;

- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

The contractor and subcontractor shall review/update them every three years, or if there is a significant change. Events that require an update to MP policy and procedures include assessments, audit findings, and security or privacy incidents.

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

20.1.1 MP-1 Return or sanitization/destruction of hard and softcopy media at the End of Performance, under the Contract.

Within three 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,
- VoIP devices,
- Hard drives,
- Router, switch, and firewall configurations,
- Network - restored to original settings, and
- 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 30 days of receipt of the plan which option is preferable. The objective of this requirement is to ensure that all SBU data, 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 and subcontractor 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.

Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), CDs, and DVDs.

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

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

20.3 MP-3 Media Marking

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

Media is exempt from marking when it remains within contractor-controlled areas.

20.4 MP-4 Media Storage

For contractors and subcontractors who maintain IRS information, the contractor and subcontractor shall physically control and securely store information system media within controlled areas. When this media contains IRS SBU data, 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 and subcontractor 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 data secured when not in use. Removable media also must be encrypted and labeled SBU data when it contains such information. For more information see the PE controls, Section 21.0 Physical and Environmental Protections.

Information system media shall be protected until the media is destroyed, or sanitized using approved equipment, techniques, and procedures.

Records shall be established to track all deposits and withdrawals from media storage facilities and libraries.

Business and functional units shall establish management controls that ensure all portable mass storage devices are inventoried, administered, and turned in during employee separations or reassignments.

This control applies primarily to media storage areas within organizations, where significant volumes of media are stored, and does not apply to every location where media are stored (e.g., in individual offices).

20.5 MP-5 Media Transport

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

Information systems shall implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. The cryptographic mechanisms in place shall be FIPS 140-2, or later compliant. This applies to both portable storage devices (e.g., USB memory sticks, CDs, DVDs, external/removable hard disk drives, SSDs) and mobile devices with storage capability (e.g., smartphones, tablets, E-readers).

Chain of custody records for digital media shall be secured to prevent unauthorized access and manipulation of log information.

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 a locked room safe, or secured in a safe, in the hotel management offices.

20.6 MP-6 Media Sanitization

The contractor and subcontractor shall sanitize information, digital, optical, and paper prior to disposal or release for reuse.

The contractor and subcontractor shall possess tools and methods to conduct sanitization of digital media that can be used in clear and purge operations as described above in 20.0 Media Protection (MP).

Optical mass storage media includes, but is not limited to: CDs, CD - rewritable (CD-RWs), CD - recordables (CD-Rs), and CD - read only memory (CD-ROMs), DVDs and magneto-optical (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 (mm) in size.

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.

IRS 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 and subcontractor authorized to perform destruction of IRS SBU data shall be approved for interim/final staff-like access or be under escort of an employee who has approved interim/final staff-like access.

Contractors using a CSP shall ensure that the CSP annually tests and verifies sanitization equipment and procedures.

20.7 MP-7 Media Use

The contractor and subcontractor shall restrict the usage of writeable removable media and prohibit the use of portable storage devices when such devices have no identifiable owner.

Add-on devices that can record, or transmit sensitive information (e.g., video, sound, Intermediate Frequency (IF), or Radio Frequency (RF)) shall be disabled in areas where sensitive information is discussed.

The contractor and subcontractor shall prohibit the usage of personally owned equipment, software, or media to process, access, or store IRS SBU data, and prohibit connecting privately-owned PED or removable media to an information system used to process, store, or transmit IRS SBU data.

21.0 Physical and Environmental Protection (PE)

Physical and environmental protection policy and procedures address the controls in the PE family that are implemented within systems and organizations. Such policies and procedures shall be developed with risk management as a focus, taking into account both security and privacy concerns. This can be a single policy document or multiple policies covering the various controls.

Physical security shall be provided for a document, an item, or an area in several 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 data as moderate risk. The controls are intended to protect the information and information systems that contain SBU data. 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 data.

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. The objective of MPS standards is to prevent unauthorized access to SBU data. MPS requires two barriers to access SBU data under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. See Appendix D for additional information on MPS and other physical security requirements.

21.1 PE-1 Physical and Environmental Protection

The contractor and subcontractor shall designate an official to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and

- Compliance.

The contractor and subcontractor shall review/update policies and procedures every three years, or if there is a significant change to physical and environmental protection procedures to be used for that contractor site. Events that require an update to PE policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws.

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 data shall also be updated at least annually. Additionally, the contractor shall have a procedure to issue, manage, and track ID cards for visitors.

Any contractor company with more than 25 total employees shall have a photo ID 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. Media used to create the badges shall be safeguarded to prevent unauthorized use. Badge access programming must be performed by an employee with interim or final staff-like access, if completed onsite. If programming is completed offsite at another contractor location, staff-like access is not required if multiple levels of approval are involved. Badges with access to any secure or limited area where SBU data is present must also have a permanent, unique identifier on the badge to visually identify employees with interim or final staff-like access.

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. All lost/stolen ID cards must be reported to management within 24 hours, or as soon as loss is identified.

Contractors using a CSP shall ensure that the CSP develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides. Review the access lists detailing authorized facility access by individuals at least annually.

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 and subcontractor 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.

Contractors using a CSP shall ensure that the CSP enforces physical access authorizations at entry/exit points to the facility where the information system resides by verifying individual access authorizations before granting access to the facility; and controlling ingress/egress to the facility using CSP defined physical access control systems/devices and guards.

See Appendix D for additional guidance on physical access controls.

21.4 PE-4 Access Control for Transmission Medium

The contractor and subcontractor 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:

- Locked wiring closets,
- Disconnected or locked spare jacks,
- Protection of cabling by conduit or cable trays, and/or
- Wiretapping sensors.

21.4.1 Transporting IRS Material

Any time SBU data is transported from one 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 when the individual is out of their hotel room, the material is to be out of view, in a locked briefcase or suitcase.

All shipments of SBU data (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 data transported through the mail or courier/messenger service shall be double-sealed; that is one 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, or later.

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 always be safeguarded during transport.

Methods to secure material shall include, but are 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; and
- 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 and subcontractor 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. Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, covering windows into secure work areas, facing output screens away from walkways, or some combination of the above.

21.6 PE-6 Monitoring Physical Access

The contractor, subcontractor, or designee shall monitor physical access to SBU data 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/potential indication of an incident. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

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.

The contractor and subcontractor shall monitor physical intrusion alarms and surveillance equipment. Closed-Circuit Television (CCTV's) shall have monitoring and recording capabilities but are not required to be monitored in real-time. Response actions can include notifying selected organizational personnel or law enforcement personnel. Automated mechanisms implemented to initiate response actions include system alert notifications, email and text messages, and activating door locking mechanisms.

21.6.1 Monitoring Private Collection Agencies (PCA)

PCA's shall have CCTV's that record all sensitive areas where taxpayer data is present, including but not limited to mail processing rooms. PCA's shall have a secure area for mail processing and securing payments, that is separate from the contractor's other mail processing. Physical security assessments of the mailrooms and mail processing sites shall be conducted annually for PCA's.

21.7 PE-8 Visitor Access Records

The contractor and subcontractor 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.

Registers or logs for all areas shall be maintained for two years.

Contractors using a CSP shall ensure that the CSP reviews visitor access logs, at least monthly.

21.8 PE-9 Power Equipment and Cabling

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

21.9 PE-10 Emergency Shutoff

The capability to shut off power to the information system or individual system components in emergency situations shall be provided. 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.

21.10 PE-11 Emergency Power

The contractor and subcontractor 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 and subcontractor 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 and subcontractor 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.

- The contractor and subcontractor 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 data in warehouse and/or storage facilities, the contractor shall ensure thatsprinkler systems and/or water suppression equipment shall be in place to minimize damage to critical historical files.

21.13 PE-14 Environmental Controls

The contractor and subcontractor shall maintain and monitor temperature levels within the facility where the information system resides. The monitoring of the temperature levels shall generate alerts or notifications when changes in temperature are potentially harmful to personnel or equipment. The alarm or notification may be an audible alarm, visual message, text or email in real time to personnel or roles defined by the organization. Such alarms and notifications can help minimize harm to individuals and damage to organizational assets by facilitating a timely incident response.

21.14 PE-15 Water Damage Protection

The contractor and subcontractor shall protect the information systems from damage resulting from water leakage by ensuring that master shutoff or isolation 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 data, the contractor and subcontractor 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. (See Appendix D for additional guidance of physical access controls of SBU and PII material, and CCTV requirements specific to PCA mail processing rooms).

21.16 PE-17 Alternate Work Site

The contractor and subcontractor shall develop procedures required to safeguard IRS SBU data for work performed at alternate work sites such as an employees' home office. A contractor management approval process shall be in place to ensure that employees working at home are aware of their responsibilities and have the ability to protect IRS SBU data. A telework agreement shall be utilized to confirm the employee's understanding and acceptance of their responsibilities for protecting data and communicating requirements for a suitable work environment.

The processing or storage of FTI is restricted to locations as prescribed in Appendix D. Namely, FTI cannot be processed or stored at employee's home or elsewhere except as otherwise approved by IRS.

Employee laptops must have full-disk encryption installed. If the computer is lost or stolen, unauthorized users will not be able to access any data on the hard drive.

Employee's working at home must report all computer security incidents to management.

Digital assistants (sometimes called smart devices) and other devices that can record or transmit sensitive audio or visual information must not be allowed to compromise privacy in the work or telework environment. These devices typically contain sensors, microphones, cameras, data storage components, speech recognition, GPS options, and other multimedia capabilities. These features could put the privacy of contractors, employees and/or taxpayers at risk due to the personal information that might be unwittingly disclosed. When working on any form of SBU data, (including PII and tax information), these rules must be followed:

- Treat the device as if it were another person in the room because many such devices and applications can record and/or transmit data when activated. To protect privacy, contractors must mute or disable the listening/detecting features of the device so that SBU data is not sent to the device or anything to which it is connected.
- If the device or application can take photos or record video or sound, then the contractor must not do sensitive work within visual or audio range.

These devices/applications include (but are not limited to the examples provided):

- Digital assistants (such as Dot or Echo hardware using Alexa software, HomePod using Siri, etc.);
- Voice-activated devices and smartphone applications (such as Siri, Google Now ("Okay Google"), or Alexa on phones, tablets, etc.);
- Internet-connected toys (Cloud Pet, Smart Toy, Hello Barbie, etc.) that might record and transmit;
- Security systems and webcams in the telework environment;
- Smart TVs or auxiliary equipment (if includes voice activation);
- Operating systems/applications (such as Windows 10, Cortana, etc.) that allow voice commands; and
- Home surveillance, security, and video/audio: Webcams on personal devices in the home, security cameras/microphones.

The employee's home environment shall have the following features/capabilities:

- A telephone;
- A workspace suitable to perform work;
- All SBU data in the possession of the employee, must be kept in a locking file cabinet or drawer;

- Secure remote network access via a VPN; and
- A work environment that is free from interruptions and provides reasonable security and protections.

22.0 Planning (PL)

The contractor and subcontractor are 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 Planning Policy and Procedures

Contractors and subcontractors shall designate an official to manage the development, documentation, and dissemination of security PL policies and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

The contractor and subcontractor shall review/update these policies and procedures every three years or if there is a significant change to formal documented requirements to complete a security PL and to address how these plans shall be updated and maintained.

22.2 PL-2 System Security and Privacy Plans

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

The SSP shall:

- Describe the operational context of the information system in terms of missions and business processes.
- Explicitly define the authorization boundary for the system.
- Identify the information types processed, stored, and transmitted by the system.
- Identify contractor personnel that fulfill system roles and responsibilities.
- Describe specific threats to that are concern to the contractor for this information system.
- Identify risk determinations for security and privacy architecture and decisions.
- Provide the results of a privacy risk assessment for systems processing PII.
- Describe the operational environment for the information system and relationships with or connections to other information systems.

- Provide an overview of the security and privacy requirements for the system.
- Describe the security and privacy controls in place or planned for meeting those requirements
- Be reviewed and approved prior to plan implementation.

The contractor or sub-contractor shall:

- Distribute copies of the security plan and communicate subsequent changes to the plan to authorized personnel.
- Review the SSP at a minimum annually or as a result of a significant change.
- Update the security plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
- Protect the SSP from unauthorized disclosure and modification.

The SSP shall include or reference a plan for media sanitization and disposition that addresses all system media and backups.

The contractor and subcontractor 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 and subcontractor shall develop a set of expected rules of behavior when processing or handling IRS SBU data. For all contractor employees who have access to IRS information, the contractor employee shall provide a signed acknowledgement indicating their understanding and expected behavior for information and system usage, security, and privacy. 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.

The contractor and subcontractor shall include in the rules of behavior, restrictions on the posting of IRS SBU data on public websites, as well as the use of IRS identifiers (e.g., email addresses) and IRS authenticators (e.g., passwords) on external sites/applications.

The contractor and subcontractor shall establish usage restrictions and implementation guidance for using internet-supported technologies (e.g., instant messaging, social media, social networking sites,) based on the potential for these technologies to cause damage, or disruption to the information system.

The use of the internet-supported technologies shall be documented, monitored, and controlled.

Any failure to comply with the rules of behavior shall be considered a security and or privacy incident. If the incident is deemed willful, it shall be escalated to a security and/or privacy violation and is subject to disciplinary actions.

22.4 PL-8 Security and Privacy Architectures

The contractor and subcontractor shall develop and maintain an information security architecture document that:

- Describes the overall security architecture of the organization;
- Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
- Describes the overall philosophy, requirements, and approach to be taken regarding 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 security architecture document shall be reviewed and updated annually to reflect updates in the enterprise architecture.

Planned information security architecture changes shall be reflected in the security and privacy plans, the security Concept of Operations (CONOPS), criticality analysis, organizational procedures, and organizational requirements that result in procurements/acquisitions.

23.0 Program Management (PM)

23.1 PM-5 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.

23.2 PM-25 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.

Fictionalize taxpayer names and addresses in training and testing materials to ensure that no taxpayer information is accidentally released, and no disclosure laws are violated.

Examples of acceptable PII fictionalization:

- For names use categories of objects, such as animals or minerals: Mr. Bass, Ms. Silver, etc.
- For Social Security Numbers, begin fictitious numbers with “0” or “X”: 000-123-4567, etc.

23.3 PM-26 Complaint Management

The contractor must notify the COR of any privacy-related complaints from the public and cooperate with any subsequent investigation.

24.0 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) to initiate appropriate background investigations. Any contractor personnel who 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 and subcontractor shall designate an official to manage the development, documentation, and dissemination of the personnel security policies and procedures and review/update them every three years, or if there is a significant change.

The policy shall define the need for all contractor personnel to obtain a favorable IRS suitability determination (interim or final staff-like access) before beginning work on any IRS contract work.

24.2 PS-2 Position Risk Designation

At the start of any contract, the Vendor POC will assist the COR with identifying position duties, level of access required, and preliminary assessments of the position risk designation for each type of position performing work on the contract. The POC/COR will complete the Position Designation Survey and return it to PS. PS inputs the position designation survey responses into OPM's Position Designation Tool to determine the correct risk level and appropriate background investigation for each type of position on the contract. The Associate Director Personnel Security has the ultimate authority for position risk designation and may adjust the risk level, if deemed appropriate. The IRS will review and update 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) 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, and/or maintain information systems, and/or require access to SBU data.

Contractors using a CSP shall assign a risk designation to all positions. Establish screening criteria for individuals filling those positions and ensure that the CSP reviews and updates position risk designations at a minimum every three years.

24.3 PS-3 Personnel Screening

Personnel screening shall take place for all contractor and subcontractor 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.

The contractor shall identify to the COR, all contractor and subcontractor staff that will:

- Work on the contract;
- Have access to or handle SBU data; or
- Have access to, operate, or work with information systems containing SBU data.

In addition, the contractor will identify which contractor and subcontractor staff has or has not completed the current annual requirements for SAT.

Call recording quality assurance staff must have approved staff-like access (interim or final).

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

24.3.1 PS-3 Eligibility

Contractor and subcontractor employees shall meet minimum citizenship requirements:

- Contractor and subcontractor employees designated as high risk must be a US citizen;
- Contractor and subcontractor employees designated as moderate risk must be a US citizen or Lawful Permanent Resident (LPR), with a minimum of three years of US residency as an LPR, and no break of US residency of a year or more;
- Contractor and subcontractor employees designated as low risk must be a US Citizen or LPR;
- Contractor and subcontractor employees must be federal tax compliant and must remain compliant for the time they are on the contract; and
- All males born after 1959 must be registered with Selective Service. If not registered or exempt, the contractor must have a Status Information Letter from Selective Service.

24.3.2 PS-3 Suitability

Suitability is defined as a person's identifiable character traits and conduct sufficient to decide whether an individual's employment or continued employment would or would not protect the integrity or promote the efficiency of the service. All contractor and subcontractor employees are subject to a background investigation to determine their suitability and fitness to work on an IRS contract, which includes access to: Treasury/bureau information; information technology and systems; facilities; and/or assets. Investigations include an FBI fingerprint screening and a variety of written, electronic, telephonic, or personal contact checks to

determine an individual's suitability and eligibility to work on federal contracts. The investigation must be favorably adjudicated.

For contractor-managed resources housing IRS information outside the IRS firewall, staff-like access shall only be granted to those contractor and subcontractor employees who have been deemed by IRS to be eligible and suitable. The contractor and subcontractor are 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 and subcontractor shall advise the IRS of any changes made to authorized personnel access privileges.

The contractor and subcontractor shall screen individuals prior to authorizing access to the information system. Only individuals who have been granted interim or final staff-like access shall be allowed access to IRS sensitive information.

24.4 PS-4 Personnel Termination

When a contractor employee or subcontractor leaves the contract, the Vendor POC, within one business day, is responsible for notifying the COR and the CO. The COR is then responsible for notifying IRS PS. The COR completes the Form 14604, Contractor Separation Checklist, and forward it to PS. PS will cancel any pending investigations or adjudications and update the security file. Even if the background investigation is already completed, notification is required so that the separation information can be appropriately recorded in the security file. The COR will verify that the subject's access to information systems is terminated, 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 COR shall gather any authenticators/credentials associated with the individual, and ensure they are terminated/revoked.

Contractors using a CSP shall ensure that the CSP disables system access within the same day of employee termination.

24.5 PS-5 Personnel Transfer

When a contractor employee or subcontractor transfers on or off the contract, the Vendor POC, within one business day, is responsible for notifying the COR and the CO. The COR is then responsible for notifying IRS PS. The Vendor POC 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 Vendor POC shall work with the COR to modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer. This shall include a new

assessment of the risk associated with the new position. If the duties of the new position are designated at a higher risk level (moving from a low-risk position to a moderate risk, or a moderate risk to a high risk), the subject must be re-investigated at the new risk level. The Vendor POC must notify the IRS COR and the CO when an employee on the contract is transferred.

Contractors using a CSP shall ensure that the CSP disables system access that is no longer required within 24 hours.

24.6 PS-6 Access Agreements

The contractor and subcontractor shall ensure that individuals requiring access to SBU data and information systems containing SBU data sign Non-Disclosure Agreements (NDA) and information system access agreements prior to being granted access to IRS SBU and shall review/update the NDAs to ensure that they are accurate and current annually.

The contractor and subcontractor shall:

- Develop and document access agreements for organizational information systems; and
- Review and update the access agreements annually.

Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

24.7 PS-7 External 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 require 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 IRS SBU data.

24.8 PS-8 Personnel Sanctions

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

Contractors using a CSP shall ensure that the CSP shall employ a formal sanctions process for personnel failing to comply with established information security and privacy policies and procedures.

25.0 PII Processing and Transparency (PT)

25.1 PT-5 Privacy Notice

The contractor shall ensure that all forms, web pages, and all other means of collecting personal information on behalf of the IRS include a Privacy Act Statement that provides formal notice to individuals from whom the information is collected.

26.0 Risk Assessment (RA)

RA controls ensure that risk can be assessed within the contractor and that appropriate mitigation controls can be implemented.

26.1 RA-1 Risk Assessment Policy and Procedures

Contractors and subcontractors shall designate an official to manage the development, documentation, and dissemination of the RA policies and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

The contractor and subcontractor shall review/update the policies and procedures every three years, or if there is a significant change to facilitate implementing RA controls. Such RA controls include risk assessments and updates to risk assessments.

26.2 RA-2 Security Categorization

In general, contracts containing SBU data 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 specifically FIPS 199.

Any information placed into an individual's calendar (e.g., Outlook,) containing SBU or PII data shall be encrypted.

26.3 RA-3 Risk Assessment

RAs are a process to identify potential threats to or vulnerabilities in the information system, and analyze what the impact to the organization is, if said threat or vulnerability occurred. The following are examples of items to be evaluated during an assessment where potential threats, or vulnerabilities may occur:

- Assignment of roles and responsibilities;
- User training;
- Assignment of elevated privileges;

- Accountability of assets;
- Supply chain;
- Remote access; and/or
- Continuity of operations.

RAs use threat sources and events as input for assessment. The following are examples of threat sources and events for assessing:

- Accounts with elevated privileges,
- Incorrect privilege settings,
- Mishandling of information by privileged users,
- Natural disasters, and/or
- Environmental failures.

For all information systems environments, an RA shall be conducted by the contractor to assess the risk and magnitude of harm that could result from 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 data and the impact of adverse effects on individuals arising from the processing of PII. In addition, an RA shall consider supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code.

The contractor and subcontractor shall integrate RA results and risk management decisions from the organization and mission or business process perspectives with system-level RAs.

The contractor shall document and review and update the RA results annually or whenever there is a significant change to the information system or environment in which it operates.

Examples of significant changes to an information system that should have an RA updated include, but are not limited to:

- Installation of a new, or upgraded OS, middleware component, or application;
- Modifications to system ports, protocols, or services;
- Installation of a new, or upgraded hardware platform or firmware component; or
- Modifications to cryptographic modules or services.

26.4 RA-5 Vulnerability Monitoring and Scanning

Vulnerability scanning is a method to inspect workstations, servers, networks, switches, routers, mobile 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, networks, mobile devices, switches, and routing devices shall undergo monthly vulnerability scanning.

Any time a contractor or subcontractor is using IT assets, such as a workstation, laptop, server, switch, router, etc., the contractor shall ensure that 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 or subcontractor is using networks, including; local area network (LAN) or wide area network (WAN), the contractor shall conduct more sophisticated network scanning methods such as; Network-based Intrusion Detection System (NIDS) or Host-based Intrusion Detection System (HIDS) 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.

The contractor and subcontractor shall use scanning tools that are SCAP validated, and that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD).

When providing programming services or hosting applications and/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 in real-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 monthly.

At the direction of IRS Cybersecurity, the contractor and subcontractor shall send monthly SCAP scan results in comma separated value (CSV) format, of all critical, high, and moderate vulnerabilities detected in the information system to the IRS COR who will share the results with Cybersecurity.

The CSV file must include the following information: the scan summary results showing the number of critical, high, and moderate vulnerabilities and the listing of critical and high vulnerabilities that include the CVE reference.

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.

Vulnerabilities shall be prioritized for remediation based on risk (highest to lowest). Newly discovered vulnerabilities shall be added to the list of vulnerabilities to be scanned prior to a new scan to ensure that the contractor will take steps to mitigate those vulnerabilities in a timely manner.

Vulnerabilities identified on the scan reports must be remediated within the following time frames:

- Critical - risk vulnerabilities shall be mitigated within 30 days from the date of discovery;
- High - risk vulnerabilities shall be mitigated within 60 days from the date of discovery; and
- Moderate - risk vulnerabilities shall be mitigated within 120 days from the date of discovery.

Scan reports shall be retained for no less than three months to support on-site security assessment trend analysis.

As part of the vulnerability remediation process, the remediating organization should identify if a vulnerability is a false positive, or not and develop a remediation plan to correct the vulnerability

Contractors using a CSP shall ensure that they or the CSP scan information systems and hosted applications (i.e., operating system/infrastructure, web applications, and databases) for vulnerabilities at least monthly and when new vulnerabilities potentially affecting the system/applications are identified and reported.

Remediate legitimate vulnerabilities using the following response times:

- High-risk vulnerabilities shall be mitigated within 30 days from date of discovery: and
- Moderate-risk vulnerabilities shall be mitigated within 90 days from date of discovery.

The contractor or CSP shall employ automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities. The CSP shall review historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

27.0 System and Services Acquisition (SA)

Information SA controls ensure that security and privacy are planned into the environment whenever IT assets are being evaluated and/or procured for use.

27.1 SA-1 System and Services Acquisition Policy and Procedures

The contractor and subcontractor shall designate an official to manage the development, documentation, and dissemination of the SA policies and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

The contractor and subcontractor shall review/update policies and procedures every three years, if there is a significant change, or following certain events including; assessment or audit findings, and security or privacy incidents; to ensure adequate information SA policies are developed and implemented.

Information assurance shall be considered a requirement for all systems used to enter, process, store, display, or transmit IRS SBU data. Information assurance provides for the availability of systems, ensures the integrity and confidentiality of information, and the authentication/non-repudiation of parties in electronic transactions.

27.2 SA-2 Allocation of Resources

The contractor and subcontractor 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 and subcontractor are managing a network or information system, they shall ensure the need for security tools is assessed as requirements are developed for procurements for IT 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.

27.3 SA-3 System Development Life Cycle (SDLC)

Whenever information systems contain SBU data, the contractor and subcontractor shall manage the information system using an information SDLC methodology that includes information security and privacy considerations.

The contractor and subcontractor shall define and document information security and privacy roles and responsibilities throughout the SDLC. Individuals with information security and privacy roles and responsibilities shall be identified.

27.4 SA-4 Acquisition Process

Information systems containing IRS SBU data shall be located and operated within the United States, its possessions, and territories. Operation and maintenance of systems shall be conducted by personnel physically located within the U.S. or its territories.

The following is prohibited:

- Foreign remote maintenance,
- Foreign systems monitoring,
- Foreign call service centers,
- Foreign help desks, and
- Foreign datacenters.

When information systems store, process, or transmit IRS SBU, the contractor and subcontractor shall include security and privacy requirements and/or security and privacy specifications on all acquisition contracts, used by the contractor.

The contractor and subcontractor shall require the developer of the information system, system component, or system service to provide design and implementation information for the security controls to be employed. These include security-relevant external system interfaces, high-level design, low-level design, source code, or hardware schematics.

Properties of security controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

The contractor and subcontractor shall ensure that systems intended to contain IRS SBU data (i.e., beyond commercial products used as components) shall be developed physically within the U.S. by U.S. citizens, or those with lawful permanent resident status.

27.6 SA-5 System Documentation

Security requirements and specifications shall be included in information system, which shall include (but not limited to) requirements such as:

- Required security capabilities,
- Development processes,
- Test and evaluation procedures,
- Required security and privacy documentation, and
- Requirements traceability.

27.7 SA-8 Security and Privacy Engineering Principles

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

Organizations apply security and privacy engineering principles primarily to newly developed information systems, or systems undergoing major upgrades. For legacy systems, organizations apply security and privacy engineering principles to system upgrades, and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems.

Security and privacy engineering principles include, for example:

- Developing layered protections;
- Establishing sound security and privacy policy, architecture, and controls as the foundation for design;
- Incorporating security and privacy requirements into the SDLC;
- Delineating physical and logical security boundaries;
- Ensuring that system developers are trained on how to build secure software;
- Tailoring security controls to meet organizational and operational needs;
- 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
- Reducing risk to acceptable levels, thus enabling informed risk management decisions.

27.8 SA-9 External System Services

The contractor and subcontractor shall require providers of external information system services to comply with information security and privacy requirements and employ appropriate security and privacy controls. Oversight of user roles and responsibilities regarding external information system services shall be defined and documented. Security and privacy control compliance by external service providers shall be monitored.

27.9 SA-10 Developer Configuration Management

The contractor and subcontractor shall require that information system developers perform configuration management during information system design, development, implementation,

operation, and disposal. Changes to the information system and the potential security and privacy impacts of such changes shall be controlled, approved, and documented. Security and privacy flaws and resolution shall be tracked.

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

27.10 SA-11 Developer Testing and Evaluation

Contractors and subcontractors who perform development work for the IRS shall ensure that testing is conducted for the development environment.

At a minimum, the contractor shall:

- Create and implement a security test and evaluation plan and privacy assessment plan;
- Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process;
- Produce evidence of the execution of the security and privacy assessment plan and the results of the security testing and evaluation.
- 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), and
    - Correct flaws identified during security testing/evaluation.

All software custom developed or configured for the IRS shall be scanned with software code vulnerability detection software before the custom software is used in support of the IRS.

27.11 SA-15 Development Process, Standards, and Tools

The contractor and subcontractor shall require the developer of an information system, system component, or information system service to follow a documented development process that:

- Explicitly addresses security and privacy requirements.
- Identifies the standards and tools used in the development process.
- Documents the specific tool options and tool configurations used in the development process.
- Documents, manages, and ensures the integrity of changes to the process and/or tools used in development.

The contractor and subcontractor shall review the development process, standards, tools, and tool options/configurations at a minimum annually, to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy IRS security and privacy requirements as defined by Publication 4812.

27.12 SA-22 Unsupported System Components

Contractors and subcontractors shall replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer or provide options for alternative sources for continued support for unsupported components such as extended support agreements with the vendor.

Information system components include, for example, mainframes, workstations, servers (e.g., database, email, authentication, web, proxy, file, domain name), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), OS, middleware, applications, and software versions. Support for information system components includes, but are not limited to: software patches, firmware updates, replacement parts, and maintenance contracts.

28.0 System and Communications Protection (SC)

Secure 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 data are protected.

28.1 SC-1 System and Communications Protection Policy and Procedures

The contractor and subcontractor shall designate an official to manage the development, documentation, and dissemination of the SC policies and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

The contractor and subcontractor shall review/update policies and procedures every three years, or if there is a significant change to ensure adequate information SC protection policies are developed and implemented.

28.2 SC-2 Separation of System and User Functionality

For all contractors and subcontractors 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.

System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. Separation of system management functions from user functions includes web administrative interfaces, that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different subnets and with additional access controls.

28.3 SC-4 Information in Shared System Resources

Contractors and subcontractors shall ensure the system prevents unauthorized and unintended information transfer via shared system resources.

This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

28.4 SC-5 Denial-of-Service Protection (DoS)

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

DoS events can be the result of an attack of a hacker or a lack of planning to support company needs with respect to capacity and bandwidth. Firewall devices can filter certain types of packets to protect system components on internal networks from being directly affected by or the source of DoS attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to DoS events.

28.5 SC-7 Boundary Protection

Contractors and subcontractors shall ensure that all internal and external information system boundaries are controlled using boundary protection mechanisms,(e.g., routers, switches).

The contractor and subcontractor shall:

- Implement subnetworks for publicly accessible system components that are physically/ logically separated from internal organizational networks;
    - Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs).
- Limit the number of external network connections to the information system.
- Implement a managed interface for each external telecommunication service;
    - Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture.
- Establish a traffic flow policy for each managed interface.
- Filter unauthorized control plane traffic from external networks;
    - External telecommunications services can provide data and/or voice communications services. Examples of control plane traffic include routing, Domain Name System (DNS), and management. Unauthorized control plane traffic can occur through a technique known as “spoofing.”
- Employ security controls as needed to protect the confidentiality and integrity of the information being transmitted across each interface.
- Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need.
- Review exceptions to the traffic flow policy annually.

- 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).
    - Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.
- The information system, in conjunction with a remote device, shall prevent the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. This is implemented within remote devices (e.g., laptop computers) through configuration settings to disable split tunneling in those devices, and in implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling.

Managed interfaces (typically using firewalls) shall be implemented and managed at trusted boundaries. Each trusted boundary shall be monitored. Communications across each boundary shall be controlled.

Configure and ensure boundary protection devices block all data coming in except through connections that are known to be trusted.

When employing firewalls for packet filtering, use stateful inspection firewalls or their equivalent, as opposed to stateless packet filtering firewalls or routers.

The capability shall exist to conduct/perform deep packet inspection (DPI) at internet access points. This capability should be placed in line, and intrusion prevention capabilities shall be utilized. Firewalls and other appropriate protection mechanisms shall be employed for wireless access points

Contractors using a CSP shall ensure that they or the CSP implement host-based boundary protection mechanisms at servers, workstations, and mobile devices.

The contractor or CSP shall isolate the information system from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

28.6 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.

Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, laptop computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios.

Unprotected communication paths are exposed to the possibility of interception and modification. Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and Internet Protocol Security (IPSec). Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

The contractor or CSP shall implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by a hardened or alarmed carrier.

28.7 SC-10 Network Disconnect

The information system shall disconnect all network connections upon session completion, or after 30 minutes of inactivity.

Applications requiring continuous, real-time screen display (e.g., network management products, certain call center workstations as defined by the company executive) shall be exempt from the network inactivity disconnect threshold provided the following requirements are met:

- The logon session was not initiated by a privileged account (e.g., root in Linux/Unix, Master in Unisys).
- The inactivity exemption is documented in the appropriate operational policy approved by the company executive; and
- The workstation is in a restricted and controlled access area open only to contractors with an approved IRS clearance.

28.8 SC-12 Cryptographic Key Establishment and Management

The contractor and subcontractor 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.

Encryption key recovery requirements, at a minimum, shall include:

- Identification of which keying material, requires backup or archive for later recovery;
- The location where backed-up or archived keying material shall be stored;
- Responsibility assignment for protecting backed-up or archived keying material;
- Required procedures for storing and recovering the keying material;

- Listing of who can request a recovery of the keying material and under what conditions;
- Listing of who will be notified when a key recovery has taken place and under what conditions; and
- Managing trust stores to ensure that only approved trust anchors are part of such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems.

The security role of an Encryption Recovery Agent shall be assigned to support recovery processes.

Encryption products shall provide for encryption key recovery to support availability needs.

Vendor-supplied default encryption keys shall be changed as soon as the system or software has been installed.

28.9 SC-13 Cryptography Protection

IRS SBU data that is processed, stored, or transmitted by a contractor or subcontractor information system shall be protected 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.

28.10 SC-15 Collaborative Computing Devices and Applications

Collaborative devices and applications 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 and applications include remote meeting devices and applications, networked white boards, cameras, and microphones.

Any implementation of a collaborative technology used in support of the contract shall be based on an assessment of risk by the Vendor POC. Collaborative computing shall not be used as a substitute for email, or other data transfer technologies.

28.11 SC-17 Public Key Infrastructure (PKI) Certificates

For all contractors and subcontractors who manage information systems, the information system shall document processes with supporting procedures for digital certificate generation, installation, and distribution. The contractor and subcontractor shall issue public key certificates under policy or procedure or obtain public key certificates from an approved service provider; and include only approved trust anchors in trust stores or certificate stores managed by the organization. Subscriber key pairs shall be generated and stored using FIPS 140-2, or later Security Level 2 or higher cryptographic modules.

Private keys are protected using, at a minimum, a strong password. Refer to Section 17.5 IA-5 Authenticator Management for strong password requirements. A certificate shall be revoked if; the associated private key is compromised, management requests revocation, or the certificate is no longer needed.

Public key infrastructure certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services. In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor. A trust store or certificate store maintains a list of trusted root certificates.

28.12 SC-18 Mobile Code

The contractor and subcontractor shall define acceptable and unacceptable mobile code and its associated technologies. Usage restrictions and implementation guidance shall be established for acceptable mobile code and its associated technologies. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including laptop computers and smartphones.

The contractor shall authorize, monitor, and control the use of mobile code within the information system.

Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript.

Mobile code policy and procedures address specific actions taken to prevent the development, acquisition, and introduction of unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.

Mobile code is a powerful computing tool that can introduce risks to the user's information system. 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.

28.13 SC-19 Voice over Internet Protocol (VoIP)

The contractor and subcontractor shall establish, document, and control usage restrictions and implementation guidance for VoIP technologies based on the potential to cause unintentional disclosure of SBU data. Appropriate contractor officials shall authorize the use of VoIP.

Call recording application systems using VoIP data packet transmissions including, but not limited to; .wav or .mp4 file, must be encrypted using Wireless Protected Access 2 (WPA2) with the Advanced Encryption Standard (AES) protocol.

VoIP phones shall not be installed or operated in publicly accessible areas.

Voice over data network implementations shall be designed with redundancy to ensure network outages do not result in the loss of both voice and data communications.

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

The contractor and subcontractor shall implement Secure Name/Address Resolution Services for systems externally accessible to the organization.

Secure Name/Address Resolution Services 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 DNS server is an example of an information system that provides name/address resolution service.

Providing authoritative source information enables external clients, including remote internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information systems that provide name and address resolution services include, for example DNS servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

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

The information systems shall request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources (e.g., DNS servers).

Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching DNS servers. DNS client resolvers either perform validation of DNSSEC signatures or clients use authenticated channels to recursive resolvers that perform such validations.

Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

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

Information systems that collectively provide name/address resolution service for an organization shall be fault tolerant and implement internal/external role separation.

Information systems that provide name and address resolution services include DNS servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Organizations typically deploy the servers in two geographically separated subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the internet).

Organizations specify clients that can access authoritative DNS servers in certain roles (e.g., by address ranges and explicit lists).

28.17 SC-23 Session Authenticity

Contractor and subcontractor information systems shall protect the authenticity of communication sessions.

Session authenticity addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of a communications session in the ongoing identities of the other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle (MITM) attacks/session hijacking and the insertion of false information into sessions.

28.18 SC-28 Protection of Information at Rest

All portable media shall be encrypted, including laptops, USB storage devices, backup tapes, internal and external hard drives, etc.

Contractors storing, processing, or transmitting IRS SBU shall employ FIPS 140-2, or later validated encryption on their primary storage devices, servers, and storage arrays. This can be accomplished via full-disk encryption or file level-based encryption.

Information at rest refers to the state of information when it is not being processed or is in transit and is located on system components. Such components include internal or external hard drives, storage area network devices, or databases. The focus of protecting information at rest is on the state of the information. Information at rest addresses the confidentiality and integrity of information and covers user information and system information.

Full-disk encryption is the process of encrypting all the data on the hard drive used to boot a computer, including the computer's OS, and permitting access to the data only after successful authentication to the full-disk encryption product. Full-disk encryption restricts access before the device is booted. Once the device is booted, full-disk encryption provides no protection at all. Therefore, it only addresses a limited set of threats. Also, full-disk encryption does not provide a fine grain protection to the files and folders as one might wish, especially if a clean separation of sensitive and non-sensitive data is not feasible.

File encryption is the process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided. Folder encryption is very similar to file encryption, only it addresses individual folders instead of files. Folder/file level encryption is transparent to applications and users can provide at rest protection for data stored in the designated files and/or folders. The folder/file level encryption can be fine grained and tuned to meet the specific encryption requirements. For example, one can specify certain types of files to be encrypted, or certain files created by different users or user roles to be encrypted.

28.19 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 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. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. This capability is available in most commercial operating systems that employ multi-state processor technologies.

29.0 System and Information Integrity (SI)

This section applies to contractors and subcontractors who are developing application programs, web-based interface applications, and/or surveys that can be completed by a user population, and other instances where input data could be manipulated, causing inaccurate information to be generated.

29.1 SI-1 System and Information Integrity Policy and Procedures

Contractors and subcontractors designate an official to manage the development, documentation, and dissemination of SI policies and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

The contractor and subcontractor shall review/update the policies and procedures every three years, or if there is a significant change to facilitate implementing SI security controls.

29.2 SI-2 Flaw Remediation

Contractors and subcontractors shall establish and implement a patch management process for all organizational information systems. Procedures shall be established for evaluating, approving, and installing patches and hot fixes to ensure patches are installed.

Patch management is a component of configuration management. Patch management includes acquiring, testing, consistently applying, and monitoring patch applications within an IT infrastructure. The process of applying and certifying the application of software patches to fix flaws is critical to sustaining the desired overall security posture for enterprise-wide IT infrastructures. Timely application of patches and the management of effective implementation and oversight processes are critical to maintaining the availability of IT systems and providing desired confidentiality and data integrity services.

Contractors and subcontractors 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.

The contractor and subcontractor shall employ automated mechanisms at least monthly to determine the state of information system components regarding flaw remediation.

The flaw remediation process shall be centrally managed.

All workstations (including laptops and mobile devices) shall be appropriately reviewed for security purposes prior to connection or reconnection to the network (e.g., checks for malicious code, updated virus protection software, critical software updates and patches, operating system integrity, disabled hardware).

Contractors using a CSP shall ensure that they or the CSP install security-relevant software and firmware updates within the time period directed by an authoritative source, or within 30 days of the update's release.

29.3 SI-3 Malicious Code Protection

The information system and/or application programs shall implement malicious code protection that includes a capability for automatic updates. The contractor and subcontractor shall centrally manage malicious code protection mechanisms.

Examples of malicious code include viruses, worms, spyware, Trojan horses, etc. The contractor shall scan weekly, 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, and mobile computing devices. Virus detection software shall be configured to perform automated updates daily, and perform automated scanning of all files, incoming and outgoing emails, and other network communications. For example: removable media, USB devices, diskettes, DVDs, or CDs, shall be scanned whenever they are connected to a computing device.

The contractor and subcontractor 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.

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 and subcontractors shall ensure they have procured and installed software to enable malicious code to be detected and acted upon.

Contractors using a CSP shall ensure that they, or the CSP implement non-signature-based malicious code detection mechanisms.

Contractors using a CSP shall ensure that they, or the CSP shall employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

Configure malicious code protection mechanisms to perform periodic scans of the information system at least weekly and real-time scans of files from external sources to include endpoints as the files are downloaded, opened, or executed.

29.3.1 Email Security

Contractors and subcontractors shall not include FTI, PII, or SBU data in email messages, or email attachments without using FIPS 140-2, or later compliant encryption.

Personal email accounts shall not be used to conduct any IRS business in performance of the contract. Use the subject line to categorize messages. Do not include any IRS SBU data in the subject line.

Contractors and subcontractors shall not post agency information whether using government furnished IT equipment, company owned, or personal resources to external news groups, bulletin boards, or other public forums without the authority of the IRS. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government Contractor.

When provided with an IRS workstation (e.g., desktop, laptop) as part of a contract, contractors shall use their IRS workstation and email account for all official communications.

Electronic messaging systems (for example, Microsoft Office, Skype for Business®, or Microsoft Teams) should only be used for informal business communications and collaborations. Contractors should not use electronic messaging systems to engage in discussions regarding policy matters, business decisions, or documentation of other mission-critical functions.

In accordance with IRM 10.8.1.3.1.18.1 *Telecommunication Devices*, the use of text messaging with government-furnished BlackBerrys, cellular phones, or smartphones to conduct official business is prohibited. Text messaging may only be used in emergencies, such as when the IRS network is down and there is an urgent need to communicate or in disaster recovery situations.

Contractors and subcontractors provisioned with government furnished equipment (GFE) and email accounts shall not send e-mail messages containing IRS information to non-government owned email accounts, except as required for work-related communications to members of the public or other third parties.

When provisioned with GFE and email accounts, automatic forwarding shall not be used to send messages to non-IRS/Treasury email accounts.

Contractors and subcontractors provisioned with GFE shall not use government furnished IT equipment or resources to access, view, or download personal email.

Contractors and subcontractors provisioned with GFE and email accounts are prohibited from generating or distributing junk email, sending or forwarding chain letters, or inappropriate messages.

Contractors and subcontractors provisioned with GFE and email accounts are specifically prohibited from using government furnished IT equipment or resources for commercial purposes, in support of "for-profit" activities and ventures, and other outside employment or business activities (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services).

29.4 SI-4 System Monitoring

The contractor and subcontractor shall employ automated tools to monitor events on the information system to: detect attacks, vulnerabilities, and to detect, deter, and report on unauthorized use of the information system.

Automated tools include, for example, host-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real-time analysis of alerts and/or notifications generated by organizational information systems.

The information system is to be monitored for unauthorized local, network, and remote connections. Events and anomalies detected by intrusion monitoring tools shall be analyzed. Whenever there is an elevated security level, the monitoring efforts shall be increased to enable deterrence, detection, and reporting to take place, so corrective actions shall be made to the networked environment. Information obtained from intrusion-monitoring tools shall be protected from unauthorized access, modification, and deletion.

All contractors and subcontractors shall ensure they have procured and installed software to enable vulnerability detection to take place.

- The contractor and subcontractor shall employ automated tools and mechanisms 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.

All internet access points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information,

A host-based monitoring mechanism shall be employed on information system components.

Contractors using a CSP shall:

- ensure that they or the CSP shall monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions.
- ensure that they or the CSP connect and configure individual intrusion detection tools into an information system-wide intrusion detection system
- ensure that the CSP employ a wireless intrusion detection to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

29.5 SI-5 Security Alerts, Advisories, and Directives

For all information systems, the contractor and subcontractor shall ensure that they receive information system security alerts/advisories on a regular basis, generate internal security alerts, advisories, and directives as deemed necessary, issue alerts/advisories to appropriate personnel, and take appropriate actions as necessary. The contractor and subcontractor shall define appropriate personnel within the organization who shall receive the alerts/advisories, and who has responsibilities to act on these.

29.6 SI-7 Software Firmware, and Information Integrity

The contractor and subcontractor shall employ integrity verification tools to information systems, which shall detect and protect against unauthorized changes to system kernels, drivers, firmware (e.g., BIOS), software (e.g., OS, applications, middleware) and security attributes.

Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). State-of-the-practice integrity checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.

The information system performs an integrity check of software, firmware, and information at:

- Startup or restart;
- The identification of a new threat to which the information system is susceptible;
- The installation of new hardware, software, or firmware; and
- At a minimum, annually.

The contractor and subcontractor shall incorporate the detection of the following into the incident response capability:

- Unauthorized changes to baseline configuration setting.
- Unauthorized elevation of system privileges.

Contractors using a CSP shall ensure that they or the CSP perform integrity checks of software, firmware, and information at:

- System startup or restart;

- The identification of a new threat to which the information system is susceptible;
- The occurrence of a security-relevant event;
- The installation of new hardware, software, or firmware; and
- At a minimum monthly.

29.7 SI-8 Spam Protection

Contractors and subcontractor shall employ and maintain up-to-date spam protection mechanisms at information system entry and exit points, mobile devices, servers, and workstations. All contractors and subcontractors shall ensure they have procured and installed software to enable spam protection within the email environment:

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

29.8 SI-10 Information Input Validation

For any applications developed by contractors or subcontractors, 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, application fuzzing, and buffer overflow.

29.9 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.

29.10 SI-12 Information Management, Retention, and Information Disposal

Contractors and subcontractors shall manage and maintain data within the information system, according to record retention standards. The IRS shall identify the record retention standards to the contractor.

Records must be maintained and managed in accordance with approved Records Control Schedules (RCS) found in General Records Schedule Document 12829, RCS Document 12990, and additional guidance provided by the contract.

The contractor must work with the IRS CO/COR to complete a Form 11671 disposal record when records have reached their final disposition and are eligible for destruction.

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.

Contractors shall ensure that all IRS data and IRS-derived data are in commercially available or open and non-proprietary format for transition in accordance with the National Archives and Records Administration (NARA) disposition guidance.

29.11 SI-16 Memory Protection

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

30.0 Supply Chain Risk Management (SR)

Supply Chain Risk Management (SCRM) ensures that contractors and subcontractors' reliance on systems and services from vendors as well as the nature of the relationships with those providers are identified. SCRM activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans.

30.1 SR-1 Supply Chain Risk Management Policy and Procedures

Contractors and subcontractors shall designate an official to manage the development, documentation, and dissemination of the SR policies and procedures.

The policies and procedures shall address:

- Purpose;
- Scope;
- Roles;
- Responsibilities;
- Management Commitment;
- Coordination among Organization Entities; and
- Compliance.

The contractor and subcontractor shall review/update the SR policies and procedures annually, or if there is a significant change.

30.2 SR-2 Supply Chain Risk Management Plan

Contractors and subcontractors shall establish and implement a SCRM plan for managing supply chain risks associated with the design, acquisition, delivery, integration, operations and maintenance, and disposal of information systems used in support of the IRS contract.

Contractors and subcontractors shall review/update the SCRM plan annually, or if there is a significant change.

The SCRM plan shall addresses management, implementation, and monitoring of SR controls and the development/sustainment of systems across the SDLC.

SCRM plans shall include an expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, a description of and justification for supply chain risk mitigation measures taken, and associated roles and responsibilities.

SCRM plans shall address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes.

30.3 SR-3 Supply Chain Controls and Processes

The contractor and subcontractor shall implement supply chain elements and processes in their SCRM.

Supply chain elements include controls or tools employed for the following:

- research and development;
- design;
- manufacturing;
- acquisition;
- delivery;
- integration;
- operations and maintenance; and
- disposal of systems and system components.

Supply chain processes include the following:

- hardware, software, and firmware development processes;
- shipping and handling procedures ;
- personnel security and physical security programs;
- configuration management tools;
- techniques;
- other programs, processes; and
- procedures associated with the development, acquisition, maintenance and disposal of systems and system components.

The contractor and subcontractor shall develop and implement a process to identify and address weaknesses or deficiencies in their supply chain controls and processes.

The contractor and subcontractor shall employ controls and processes to protect against supply chain risks to the information system, system components, or system services, and to limit the harm or consequences from supply chain-related events.

30.4 SR-5 Acquisition Strategies, Tools, and Methods

The contractor and subcontractor shall develop and implement acquisition strategies and methods to protect against, identify, and mitigate supply chain risks.

The contractor and subcontractor shall provide awareness training to employees about supply chain risk and available mitigation strategies.

The results from a supply chain risk assessment can guide and inform the strategies, tools, and methods that are most applicable to the contractor's environment. Tools and techniques may provide protection against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the SDLC.

30.5 SR-6 Supplier Assessments and Reviews

The contractor and subcontractor shall annually assess and review the supply chain-related risks associated with suppliers and the information system, system components, or system services provided.

An assessment and review of supplier risk includes security and SCRM processes, foreign ownership control or influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers.

The reviews may be conducted by the organization or by an independent third party. The reviews consider documented processes, documented controls, all-source intelligence, and publicly available information related to the supplier. Organizations can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits.

30.6 SR-8 Notification Agreements

The contractor and shall notify the IRS COR, CO, and the CSIRC Incident Response Operations Team at (240) 613-3606 24x7x365 immediately upon discovery of a potential Supply Chain Attack/Compromise that effects an information system and/or system component that supports the IRS contract.

The contractor and subcontractor shall ensure that agreements and procedures are established with entities involved in the supply chain for the system, system components, or system services for notification of supply chain compromises and results of assessments or audits.

The establishment of agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected information systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

30.7 SR-10 Inspection of Systems or Components

The contractor and subcontractor shall inspect information systems or system components when removed from contractor-controlled areas or when there may have been a potential security incident.

The inspection of systems or system components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components removed from contractor-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, entity in which the part is purchased, and when individuals return from travel to high-risk locations.

30.8 SR-11 Component Authenticity

The contractor and subcontractor shall develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system. Anti-counterfeiting policies and procedures support tamper resistance and provide a level of protection against the introduction of malicious code.

The contractor and subcontractor shall train personnel with relevant roles to detect counterfeit system components including hardware, software, and firmware. Sources of counterfeit components include manufacturers, developers, vendors, and counterfeit websites.

The contractor and subcontractor shall maintain configuration control over the system components awaiting service or repair and serviced or repaired components awaiting return to service.

30.9 SR-12 Component Disposal

The contractor and subcontractor shall dispose of software code, documentation, tools, or system components using IRS approved techniques and methods. Software code, documentation, tools, or system components can be disposed of at any time during the SDLC (not only in the disposal or retirement phase of the life cycle).

Disposal can occur during research and development, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, and partial reuse of components. Opportunities for compromise during disposal affect physical and logical data including system documentation, portable media with software code; or routers or servers that include permanent storage which contain IRS SBU data.

31.0 Privacy

Agencies and the contractors acting on their behalf must abide by NIST SP 800-53 Rev. 5. All privacy controls are initially assessed in the PCLIA and subsequently through the contractor site visits.

In addition to the privacy controls in this publication, IRM 10.5.1 outlines the IRS Privacy Principles and establishes the minimum baseline privacy policy and requirements for all IRS SBU data (including PII and FTI) to:

- Establish and maintain a comprehensive privacy program;
- Comply with privacy requirements and manage privacy risks;
- Ensure the protection and proper use of SBU data of the IRS;
- Prevent unauthorized access to SBU data of the IRS; and
- Enable operation of IRS environments and business units that meet the requirements of this policy and support the business needs of the organization.

The following publicly available sections of IRM 10.5.1 apply to the contractor (included under the term "IRS personnel") and are available at:
(https://www.irs.gov/irm/part10/irm_10-005-001)

10.5.1.1 - Program Scope and Objectives
10.5.1.1.1 - Purpose of the Program
10.5.1.1.2 - Audience
10.5.1.1.3 - Policy and Program Owners
10.5.1.1.4 - Primary Stakeholders
10.5.1.1.5 - Background
10.5.1.1.6 - Authority
10.5.1.2 - Key Privacy Definitions
10.5.1.2.1 - Privacy Lifecycle
10.5.1.2.2 - Sensitive But Unclassified (SBU) Data
10.5.1.2.2.1 - Examples of SBU data
10.5.1.2.2.2 - Official Use Only and Limited Official Use
10.5.1.2.2.3 - Freedom of Information Act (FOIA) and SBU data
10.5.1.2.3 - Personally Identifiable Information (PII)
10.5.1.2.3.1 - Examples of PII
10.5.1.2.3.2 - Public Record
10.5.1.2.3.3 - Defining PII versus Sensitive PII
10.5.1.2.4 - Tax Information
10.5.1.2.5 - UNAX
10.5.1.2.6 - Unauthorized Access of SBU data
10.5.1.2.7 - Privacy Act Information
10.5.1.2.8 - Need To Know
10.5.1.3 - Key Privacy Concepts
10.5.1.3.1 - Privacy Controls
10.5.1.3.2 - IRS Privacy Principles
10.5.1.3.2.1 - Accountability [PVR-01]

10.5.1.3.2.2 - Purpose Limitation [PVR-02]
10.5.1.3.2.3 - Minimizing Collection, Use, Retention, and Disclosure [PVR-03]
10.5.1.3.2.4 - Openness and Consent [PVR-04]
10.5.1.3.2.5 - Strict Confidentiality [PVR-05]
10.5.1.3.2.6 - Security [PVR-06]
10.5.1.3.2.7 - Data Quality [PVR-07]
10.5.1.3.2.8 - Verification and Notification [PVR-08]
10.5.1.3.2.9 - Access, Correction, and Redress [PVR-09]
10.5.1.3.2.10 - Privacy Awareness and Training [PVR-10]
10.5.1.4 - Service wide Privacy Roles and Responsibilities
10.5.1.4.1 - Employees/Personnel
10.5.1.4.2 - Management
10.5.1.4.3 - Senior Management/Executives
10.5.1.4.4 - System Owners
10.5.1.4.5 - System Developers
10.5.1.4.6 - Authorizing Officials
10.5.1.4.7 - Personnel Engaged in Procurement Activities
10.5.1.5 - Privacy Culture
10.5.1.5.1 - Clean Desk Policy
10.5.1.5.2 - Privacy in Practice (PiP)
10.5.1.6 - Practical Privacy Policy
10.5.1.6.1 - Protecting and Safeguarding SBU data and PII
10.5.1.6.1.1 - Deciding Risk Levels for SBU data and PII
10.5.1.6.1.2 - Limiting Sharing of SBU data and PII
10.5.1.6.1.3 - Extracting SBU data (Including PII and Tax Information)
10.5.1.6.2 - Encryption
10.5.1.6.2.1 - External
10.5.1.6.2.2 - Internal
10.5.1.6.2.3 - Attachment Encryption Instructions
10.5.1.6.3 - Computers and Mobile Computing Devices
10.5.1.6.4 - Data Loss
10.5.1.6.5 - Marking
10.5.1.6.6 - Storage
10.5.1.6.7 - Transmission
10.5.1.6.7.1 - Field and Travel
10.5.1.6.7.2 - Mail
10.5.1.6.7.3 - Shipping
10.5.1.6.7.4 - Faxing
10.5.1.6.7.5 - Phone
10.5.1.6.7.6 - Text Messaging (Texting)
10.5.1.6.7.7 - Electronic
10.5.1.6.7.8 - Information Privacy During Office Moves
10.5.1.6.8 - Email
10.5.1.6.8.1 - Emails to Taxpayers and Representatives
10.5.1.6.8.2 - Emails to Other External Stakeholders
10.5.1.6.8.3 - Emails to IRS Accounts
10.5.1.6.8.4 - Emails with Personal Accounts
10.5.1.6.8.5 - Limited Exceptions to Email SBU data Encryption

10.5.1.6.8.6 - Surveys by Email
10.5.1.6.9 - Disposition and Destruction
10.5.1.6.9.1 - Recycling
10.5.1.6.10 - Global Positioning Systems (GPS)
10.5.1.6.11 - Telework
10.5.1.6.12 - Bring Your Own Device (BYOD)
10.5.1.6.13 - Civil Liberties
10.5.1.6.13.1 - First Amendment
10.5.1.6.13.2 - Recordings in the Workplace
10.5.1.6.13.3 - Monitoring Individuals
10.5.1.6.14 - Contractors
10.5.1.6.15 - Online Data
10.5.1.6.15.1 - Electronic Authentication (e-Authentication)
10.5.1.6.15.2 - IRS.gov
10.5.1.6.15.3 - Intranet
10.5.1.6.16 - Social Media
10.5.1.6.17 - Collaborative Data
10.5.1.6.17.1 - Outlook Calendar
10.5.1.6.17.2 - Online Meeting Tools
10.5.1.6.17.3 - Shared Drives
10.5.1.6.17.4 - SharePoint
10.5.1.6.17.5 - Cloud Computing
10.5.1.6.18 - Training
10.5.1.7 - Introduction to Privacy-Related Programs
10.5.1.7.1 - IRS Privacy Council
10.5.1.7.2 - Privacy and Civil Liberties Impact Assessment (PCLIA)
10.5.1.7.3 - Business PII Risk Assessment (BPRA)
10.5.1.7.4 - Treasury PII Holdings Report
10.5.1.7.5 - Unauthorized Access (UNAX)
10.5.1.7.6 - Mandatory Briefings
10.5.1.7.7 - Records and Information Management (RIM)
10.5.1.7.8 - Disclosure
10.5.1.7.9 - Electronic Risk Assessment (e-RA)
10.5.1.7.10 - Enterprise Life Cycle (ELC)
10.5.1.7.11 - IT Security
10.5.1.7.12 - Incident Management (IM)
10.5.1.7.13 - Pseudonym
10.5.1.7.14 - Social Security Number Elimination and Reduction (SSN ER)
10.5.1.7.14.1 - Acceptable Use of SSNs
10.5.1.7.14.2 - SSN Necessary-Use Criteria
10.5.1.7.15 - SBU data Use
10.5.1-1 - Glossary and Acronyms
10.5.1-2- References

32.0 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.

A completed Form 14604, Contractor Separation Checklist is required. This checklist is used to separate a contractor from an IRS contract, and to document the return of all security items, Government property, and information/records to the appropriate office.

Contractors shall confirm to IRS officials that information furnished under the contract has been properly returned, disposed of, or destroyed. 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 data is always protected during transport.

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

All VoIP shall be sanitized prior to returning to production, when SBU data 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.

32.1 Destruction or Return of SBU data

When the contract is officially closed out, SBU data 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.

See Section 20.0 Media Protection, concerning Media Transport and Media Sanitation.
See Section 29.10 SI-12 Information Management, Retention, and Information Disposal, concerning transfer of data to IRS.

Contractors shall follow the IRS Records Control Schedules (RCS), Document 12990 and General Records Schedules (GRS), Document 12829 for NARA approved records retention

and destruction authorization applicable to their IRS business use. 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 the destruction of the media, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, cross-cut shredding, incinerating, pulverizing, and melting.

Either an IRS employee or a contractor with IRS approved interim/final staff-like access shall be present during the incineration and/or destruction of SBU data. The employee shall be present and observe the destruction process.

33.0 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 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 of 1997 apply to all contractors, and contractor employees. Before any contractor employee can be given access to returns, they shall have been approved for interim/final staff-like access by IRS PS 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 CO or designee. UNAX forms shall not be retained at the contractor site.

UNAX deals with the unauthorized access. UNAX also addresses any inadvertent access (accidental) made by an employee or a contractor.

Contractors shall ensure that no tax return information is disclosed to any person not authorized to access the information. IRC Section 7213 covers unauthorized disclosure of information. Unauthorized disclosure of tax return information is a felony.

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 1 - Legal Requirements and Exhibit 2 – Taxpayer Browsing Protection Act).

Contractors shall make their 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.

Exhibit 1 Legal Requirements

IRC Section 7213 Unauthorized Disclosure of Information

Federal Employees

It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)]. **Any violation of this paragraph shall be a felony** punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

Other Persons

It shall be unlawful for any person to whom any return or return information [as defined in section 6103(b)] is disclosed in a manner not authorized by this title thereafter to willfully print or publish in any manner not provided by law any such return or return information. **Any violation of this paragraph shall be a felony** punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

Solicitation

It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information [as defined in 6103(b)] and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

Section 7213A Unauthorized Inspection of Returns or Return Information

Federal Employees and Other Persons

It shall be unlawful for (A) any officer or employee of the United States, or (B) any person described in section 6103(n) or an officer willfully to inspect, except as authorized in this title, any return or return information.

Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding $1000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

For purposes of this section, the terms "inspect", "return", and "return information" have respective meanings given such terms by section 6103(b).

Exhibit 2 Taxpayer Browsing Protection Act

IRC Section 7431 Civil Damages for Unauthorized Inspection or Disclosure of Returns and Return Information.

Inspection or Disclosure by a Person Who is Not an Employee of the United States

If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against such person in a district court of the United States.

Damages

In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of

(1) The greater of-

A. $1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

B. The sum of-

i. the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus
ii. in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) The cost of the action.

(3) Subparagraph (B) of section 1030(a)(2) of title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

Definitions

For purposes of this section, the terms "inspect", "inspection", "return" and "return information" have the respective meanings given such terms by section 6103(b).

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
BOD	Business Operating Division
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
CO	Contracting Officer
CONOPS	Concept of Operations
COR	Contracting Officer's Representative
COTS	Commercial Off the Shelf Software
CP	Contingency Planning
CSA	Contractor Security Assessments
CSIRC	Computer Security Incident Response Center
CSP	Cloud Service Provider
DM	Data Minimization and Retention
DVD	Digital Video Device
FAR	Federal Acquisition Regulation
FAX	Facsimile Machines
FDE	Full-Disk Encryption
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act 2002. Amended 2014

Acronym	Acronym Description
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
GRS	General Records Schedules
GSA	General Services Administration
HIDS	Host-Based Intrusion Detection System
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
LAN	Local Area Network
LES	Law Enforcement Sensitive
MA	Maintenance
MAC	Media Access Control
MO	Magneto-Optical
MP	Media Protection
MPS	Minimum Protection Standards
NARA	National Archives and Records Administration
NAT	Network Address Translation
NET	Networked Information Technology
NIDS	Network-Based Intrusion Detection System
NIST	National Institute of Standards and Technology
OEP	Occupant Emergency Plan
OMB	Office of Management & Budget
PCLIA	Privacy and Civil Liberties Impact Assessment
PE	Physical & Environmental Protection
PED	Personal Electronic Device

Acronym	Acronym Description
PGLD	Privacy, Governmental Liaison and Disclosure
PKI	Public Key Infrastructure
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PL	Planning
PM	Program Management
POA&M	Plan of Actions and Milestones
POC	Point of Contact
PS	Personnel Security
PTA	Privacy Threshold Analysis
RA	Risk Assessment
RAC	Risk Assessment Checklist
RCS	Records Control Schedules
RIM	Records and Information Management
ROM	Read Only Memory
RPO	Recovery Point Objective
RTO	Recover Time Objective
SA	System and Services Acquisition
SA&A	Security Assessment & Authorization
SAMC	Situational Awareness Management Center
SBU	Sensitive But Unclassified
SC	System and Communication Protection
SCAP	Security Content Automation Protocol
SI	System and Information Integrity
SOFT	Software Application Development or Maintenance
SP	Special Publication
SQL	Structured Query Language
SR	Supply Chain Risk Management
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

Access Control: The process of granting or denying specific requests to: 1) obtain and use information and related information processing services, and 2) enter specific physical facilities (e.g., Contractor Facilities).

Account Manager: User account management involves the process of requesting, establishing, issuing, modifying, and closing user accounts; tracking users and their access authorization and privileges.

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.

Authenticator: The means used to confirm the identity of a user, processor, or device (e.g., user password or token).

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.

Breach: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) a person accesses or potentially accesses personally identifiable information for an unauthorized purpose (i.e., a purpose unrelated to their official duties/functions).

C

Classified Information: National security information classified pursuant to Executive Order 12958.

Cloud Service Provider: A cloud service provider is a company that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses or individuals.

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.

Continuous Monitoring: Maintaining an ongoing awareness to support organizational risk decisions.

Contingency Plan: Management policy and procedures used to guide an contractor response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the contractor to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions.

Contracting Officer's Representative: As defined in FAR Part 2, the COR means an individual, designated and authorized in writing by the CO 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.

COTS: Commercial off the shelf

Counter Measures: 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.

CSIRC: Computer Security Incident Response Center

D

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

Data At Rest: All data in computer storage (e.g., on hard disk drives, CDs/DVDs, floppy disks, thumb drives, PDAs, cellphones, other removable storage media, etc.) while excluding data that is traversing in a network (data in transit) or temporarily residing in computer memory to be read or updated (data in use).

Disaster Recovery Plan: A written plan for recovering one or more systems at an alternate facility in response to a major hardware or software failure or destruction of facilities

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

De-militarized Zone: Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Denial of Service: The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Digital Certificate: A digital representation of information used in conjunction with a public key encryption system, which at a minimum: 1) Identifies the certification authority issuing it; 2) Names or identifies its subscriber; 3) Contains the subscriber's public key; 4) Identifies its operational period. 5) Is digitally signed by the certification authority issuing it.

Disclosure: The making known to any person in any manner whatever a return or return information. See IRC 26 U.S.C. § 6103(b)(8) for the statutory definition of disclosure.

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: Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

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

Federal Tax Information: Any return or return information received from the IRS or secondary source, such as SSA etc. FTI includes any information created by the recipient that is derived from return or return information. (Internal Revenue Code (IRC) § 6103, confidentiality and disclosure of returns and return information.)

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.

FMSS: Facilities Management and Security Services

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

Information Assurance: Measures that protect and defend information and systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of systems by incorporating protection, detection, and reaction capabilities

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.

Incident: An occurrence that one, actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or a system; or two, constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Incident Response Plan: The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyber-attacks against an organization's systems.

Interconnection Security Agreement: An agreement established between organizations that own and operate connected IT systems to document the technical requirements of the interconnection.

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.

Mass Storage Device: A storage drive: hard disk, solid state disk, or USB drive that makes it possible to store and port large amounts of data across computers, servers and within an IT environment.

Media: There are two primary types of media in common use: Hard copy media are physical representations of information, most often associated with paper printouts. However, printer and facsimile ribbons, drums, and platens are all examples of hard copy media. Electronic (i.e., "soft copy") are devices containing bits and bytes such as
hard drives, random access memory (RAM), read-only memory (ROM), disks, flash memory, memory devices, phones, mobile computing devices, networking devices.

Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA): A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/MOA defines the

responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.

Mobile Code: Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.

Multi-factor Authentication: Requires using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (i.e., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

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.

NIST: National Institute of Standards and Technology

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: Per OMB Circular A-130: "Personally identifiable information' means information that can be used to distinguish or trace an individual's identity,

either alone or when combined with other information that is linked or linkable to a specific individual.

Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency *(in this case, the contractor on behalf of the IRS)* shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available – in any medium and from any source – that would make it possible to identify an individual.
Circular A-130, page 33:

https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

PGLD: Privacy, Governmental Liaison and Disclosure

Plan of Actions and Milestones: 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 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.

Privileged Account: An account with elevated privileges.

Privacy Threshold Analysis: An abbreviated analysis used to identify and document any additional privacy compliance requirements and can be used to determine whether a full PCLIA is needed.

Public Key Infrastructure: 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.

Remote Maintenance: Maintenance activities conducted by individuals communicating external to a system security perimeter.

Removable Media: Any type of storage device that can be removed from a computer while the system is still running. Examples include CDs, DVDs, diskettes, and USB drives.

Residual Risk: Portions of risk remaining after security controls or countermeasures are applied.

Returns and Return Information: Any information defined by IRC, 26 U.S.C. § 6103(b). Tax information from IRS business processes come under many names, such as FTI, IRC § 6103-protected information, taxpayer data, taxpayer information, tax return information, return information, case information, SBU data, and PII. See 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 identifying 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.

Sanitization: Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

SCADA: Supervisory Control and Data Acquisition.

Security Content Automation Protocol: A method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements.

Security Information and Event Management: A tool/application that provides the ability to gather security data from system components and present that data as actionable information via a single interface.

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: 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.

Service Level Agreement: Defines the specific responsibilities of the service provider and sets the customer expectations.

Significant Change: Also referred to as major change – A change that is likely to affect the security state of a system.

Staff-Like Access: Staff-Like Access is the authority granted to perform one or more of the following:

- Enter IRS facilities or space (owned or leased) unescorted (when properly badged);
- Possess login credentials to information systems (IRS or vendor-owned systems that store, collect, and/or process IRS information);
- Possess physical and/or logical access to (including the opportunity to see, read, transcribe, and/or interpret) Sensitive but Unclassified (SBU) data, wherever the location; (See IRM 10.5.1 for examples of SBU data);
- Possess physical access to (including the opportunity to see, read, transcribe, and/or interpret) security items and products (e.g., items that must be stored in a locked container, security container, or a secure room, wherever the location. These items include, but are not limited to security devices/records, computer equipment, Identification media. For details and further security requirements, see IRM 1.4.6.3.1, Minimum Protection Standards); or
- Enter physical areas, wherever the location, that store/process SBU data (unescorted).

Staff-Like Access is granted to an individual who is not an IRS employee (and includes, but is not limited to: contractors/subcontractors, whether procured by IRS or another federal agency, vendors, delivery persons, experts, consultants, paid/unpaid interns, other federal employees,

cleaning/maintenance employees, etc.), and is approved upon required completion of a favorable suitability/fitness determination conducted by IRS PS.

Suitability: A person's identifiable character traits and conduct sufficient to decide whether an individual's employment or continued employment would or would not protect the integrity or promote the efficiency of the service.

System Development Life Cycle: The scope of activities associated with a system, encompassing the system's initiation, development, and acquisition, implementation, operation, and maintenance, and ultimately its disposal that instigates another system initiation.

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.

Trusted Network: The networks inside an organization's security perimeter.

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

Vendor Point of Contact: The POC 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.

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

Virtual Private Network: A virtual network, built on top of existing physical networks that provide a secure communications tunnel for data and other information transmitted between networks.

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.

W

Whitelist: A list of hosts or applications that are known to be benign and are approved for use within an organization and/or system.

X

Y

Z

Appendix C: Security Control Levels

All contractors are required to use the applicable Security Control Levels to ensure the protection of IRS SBU data and information systems, including contracting actions using Simplified Acquisition Procedures. If and when additional controls are required, these shall be defined in the solicitation/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 of this appendix serves as a quick reference guide on the conditions and operators typical for each security control level within a hierarchy.

Table 5 – Table of Security Controls identifies the specific security controls applicable to each security control level.

Legend

The "high water" mark concept employs a hierarchy that goes from the least stringent security control. It considers several risk-based factors with due deference to higher risk factors (operators) such as networked environments and software development).

Figure 1 Security Control Level High Water Mark

Networked Information Technology Infrastructure (NET)
Software Application Development or Maintenance (SOFT)

Software Application Development or Maintenance (**SOFT**)	**N**etworked **I**nformation **T**echnology Infrastructure (**NET**)
Contracting actions for services that involve contractor access to SBU data 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 SOFT security controls. Other conditions and factors determine the need for additional security controls.	Contracting actions for services that involve contractor access to SBU data 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 NET security controls. Other conditions and factors determine the need for additional security controls.

Table 5: Security Controls Table

NIST CONTROL	Networked Information Technology Infrastructure (NET)	Software Application Development or Maintenance (SOFT)
AC-1 Access Control Policy and Procedures	X	X
AC-2 Account Management	X	X
AC-3 Access Enforcement	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
AC-8 System Use Notification	X	X
AC-11 Device Lock	X	X
AC-12 Session Termination	X	X
AC-14 Permitted Actions without Identification or Authentication	X	X
AC-17 Remote Access	X	X
AC-18 Wireless Access	X	X
AC-19 Access Control for Mobile Devices	X	X
AC-20 Use of External Systems	X	X
AC-21 Information Sharing	X	X
AC-22 Publicly Accessible Content	X	X
AT-1 Awareness and Training Policy and Procedure	X	X
AT-2 Literacy Training and Awareness	X	X
AT-3 Role Based Training	X	X
AT-4 Training Records	X	X
AU-1 Audit and Accountability Policy and Procedures	X	X
AU-2 Event Logging	X	X
AU-3 Content of Audit Records	X	X
AU-4 Audit Log Storage Capacity	X	X
AU-5 Response to Audit Logging Processing Failures	X	X
AU-6 Audit Record Review, Analysis, and Reporting	X	X
AU-7 Audit Record Reduction and Report Generation	X	X
AU-8 Time Stamps	X	X

AU-9 Protection of Audit Information	X	X
AU-11 Audit Record Retention	X	X
AU-12 Audit Record Generation	X	X
CA-1 Assessment, Authorization, and Monitoring Policies and Procedures		X
CA-2 Control Assessments		X
CA-3 Information Exchange	X	X
CA-5 Plan of Action and Milestones	X	X
CA-6 Authorization	X	X
CA-7 Continuous Monitoring	X	X
CA-9 Internal System Connections	X	X
CM-1 Configuration Management Policy and Procedures	X	X
CM-2 Baseline Configuration	X	X
CM-3 Configuration Change Control	X	X
CM-4 Impact Analysis	X	X
CM-5 Access Restrictions for Change	X	X
CM-6 Configuration Settings	X	X
CM-7 Least Functionality	X	X
CM-8-System Component Inventory	X	X
CM-9 Configuration Management Plan	X	X
CM-10 Software Usage Restrictions	X	X
CM-11 User-Installed Software	X	X
CM-12 Information Location	X	X
CP-1 Contingency Planning Policy and Procedures	X	X
CP-2 Contingency Plan	X	X
CP-3 Contingency Training	X	X
CP-4 Contingency Plan Testing	X	X
CP-6 Alternate Storage Site	X	X
CP-7 Alternate Processing Site	X	X
CP-8 Telecommunications Services	X	X
CP-9 System Backup	X	X
CP-10 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
IA-3 Device Identification and Authentication	X	X
IA-4 Identifier Management	X	X
IA-5 Authenticator Management	X	X

IA-6 Authenticator Feedback	X	X
IA-7 Cryptographic Module Authentication	X	X
IA-8 Identification and Authentication (Non- Organizational Users)	X	X
IR-1 Incident Response Policy and Procedures	X	X
IR-2 Incident Response Training	X	X
IR-3 Incident Response Testing	X	X
IR-4 Incident Handling	X	X
IR-5 Incident Monitoring	X	X
IR-6 Incident Reporting	X	X
IR-7 Incident Response Assistance	X	X
IR-8 Incident Response Plan	X	X
MA-1 Maintenance Policy and Procedures	X	X
MA-2 Controlled Maintenance	X	X
MA-3 Maintenance Tools	X	X
MA-4 Non-Local Maintenance	X	X
MA-5 Maintenance Personnel	X	X
MA-6 Timely Maintenance	X	X
MP-1 Media Protection Policy and Procedures	X	X
MP-2 Media Access	X	X
MP-3 Media Marking	X	X
MP-4 Media Storage	X	X
MP-5 Media Transport	X	X
MP-6 Media Sanitization	X	X
MP-7 Media Use	X	X
PE-1 Physical and Environmental Protection	X	X
PE-2 Physical Access Authorizations	X	X
PE-3 Physical Access Control	X	X
PE-4 Access Control for Transmission Medium	X	X
PE-5 Access Control for Output Devices	X	X
PE-6 Monitoring Physical Access	X	X
PE-8 Visitor Access Records	X	X
PE-9 Power Equipment and Power Cabling	X	X
PE-10 Emergency Shutoff	X	X
PE-11 Emergency Power	X	X
PE-12 Emergency Lighting	X	X
PE-13 Fire Protection	X	X
PE-14 Environmental Controls	X	X

PE-15 Water Damage Protection	X	X
PE-16 Delivery and Removal	X	X
PE-17 Alternate Work Site	X	X
PE-18 Location of Information System Components	X	X
PL-1 Planning Policy and Procedures	X	X
PL-2 System Security and Privacy Plans	X	X
PL-4 Rules of Behavior	X	X
PL-8 Security and Privacy Architectures	X	X
PM-5 Inventory of Personally Identifiable Information	X	X
PM-25 Minimization of PII used in testing, training, research	X	X
PM-26 Complaint Management	X	X
PS-1 Personnel Security Policy and Procedures	X	X
PS-2 Position Categorization	X	X
PS-3 Personnel Screening	X	X
PS-4 Personnel Termination	X	X
PS-5 Personnel Transfer	X	X
PS-6 Access Agreements	X	X
PS-7 External Personnel Security	X	X
PS-8 Personnel Sanctions	X	X
PT-5 Privacy Notice	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 Monitoring and Scanning	X	X
SA-1 System and Security Acquisition Policy and Procedures	X	X
SA-2 Allocation of Resources	X	X
SA-3 System Development Life Cycle	X	X
SA-4 Acquisition Process	X	X
SA-5 System Documentation		X
SA-8 Security and Privacy Engineering Principles		X
SA-9 External System Services	X	X
SA-10 Developer Configuration Management		X
SA-11 Developer Security Testing and Evaluation		X

SA-15 Development Process, Standards, and Tools		X
SA-22 Unsupported System Components	X	X
SC-1 System and Communications Protection Policy and Procedures	X	X
SC-2 Separation of System and User Functionality	X	X
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
SC-15 Collaborative Computing Devices and Applications		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 Resolution Service	X	X
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
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 Management, Retention, and Disposal	X	X
SI-16 Memory Protection	X	X
SR-1 Supply Chain Risk Management Policy and Procedures	X	X
SR-2 Supply Chain Risk Management Plan	X	X
SR-3 Supply Chain Controls and Process	X	X
SR-5 Acquisition Strategies, Tools, and Methods	X	X
SR-6 Supplier Assessments and Reviews	X	X
SR-8 Notification Agreements	X	X
SR-10 Inspection of Systems or Components	X	X
SR-11 Component Authenticity	X	X
SR-12 Component Disposal	X	X

Appendix D: Physical Access Control Guidelines

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 data during duty and non-duty hours. This can be accomplished by creating limited areas, security rooms, or locked rooms. Additionally, SBU data 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 data. MPS requires two barriers to access SBU data 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 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 data. A security guard shall have access to a locked building or a locked room if SBU data is in a locked container. If SBU data 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 data. 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 data. IT information systems and media shall be committed to or configured to restrict access to SBU data. The contractor shall retain ownership and control for all hardware, software, and telecommunications equipment used to handle and process, access and store SBU data.

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 homework sites, remote terminals, or office work sites where all 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 data locked up when not in use. Removable media also shall be labeled SBU data when they contain such information. Removable
media also must be encrypted and labeled SBU data when it contains such information.

In instances where encryption is not used, the contractor and subcontractor 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 data shall be clearly labeled as SBU data 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:

Table 4: Protection Alternative Chart

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

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 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 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 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 been granted interim or final staff-like access by Personnel Security and 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'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 who have been granted interim or final staff-like access by Personnel Security and 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 staff-like access during duty and non-duty hours.

Access to containers containing SBU information shall be restricted to employees who have an IRS approved staff-like access. 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; and
- The contractor shall develop a clean desk policy that requires all employees to secure SBU data after work hours, during extended absence from work such as lunch, or when employee is not immediately working with the SBU data. The clean desk policy must be communicated to all employees.

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 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 data.

The contractor shall control all access points to the 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 limited 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 limited access area register shall be maintained at a designated entrance to the limited 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 limited 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 Limited 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 staff-like access that have access to information systems or areas, where SBU data 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 secured 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 secured or protected areas must have either internal door hinges or hinges that are tamper resistant.
- Limited access areas shall have signs prominently posted as "Limited 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 Limited Area Access.
- A limited access area register will be maintained at the main entrance of each limited area, and all visitors will be directed to the main entrance. Each person entering a limited area, who is not assigned to the area, will be required to sign the register.
- The limited 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 Limited 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 Limited Access Area Register will be closed out at the end of each month, reviewed by the limited area first line supervisor and forwarded to their manager. The manager will review the register and retain it for at least two year. The managerial review is designed to ensure that only authorized individuals with an official need have access to the limited areas.

- To facilitate the entry of employees who have a frequent and continuing need to enter a limited area, an Authorized 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 Limited Access Area Register.

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

Locking Systems for Secure and Limited 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 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. All mail processing areas must have CCTV coverage:

CCTV -

- Purpose: The purpose of a CCTV system is designed to reduce risk and to assist with the deterrence, detection, surveillance, and investigation of incidents or potential incidents relevant to the protection of personnel information and facilities.
- Guiding CCTV Principles: In planning, implementing and/or revising of the CCTV system, surveillance as it pertains to deterrence, investigation and detection must be based on the following guiding principles:

    - Risk: Ensure that appropriate visual coverage exists throughout the facility and carefully consider high risk areas. For PCA's, the area where incoming mail

potentially containing remittances is opened is considered critical. Any storage of unopened mail or remittances would also be considered critical. High risk areas would include data centers/server rooms and primary ingress/egress points. Other areas would qualify as low risk. For print vendors, high risk areas would include data centers/server rooms, printing and inserting areas, primary ingress/egress points, and dock areas where large volumes of letters are stored awaiting transport. Other areas would qualify as low risk.

- High vs. Low-Risk Areas: Avoid wide angle coverage of individual work areas where an audit trail has yet to be established. Concentrate direct coverage on individual workspace such as in extraction. Use more of a broader surveillance approach or less cameras in lower risk areas.
- Recognition: Structure views to the extent that an individual may be personally recognized when entering/exiting interior mail processing areas even though it may be necessary to get a full shot of the doorway to guard against paper/information being passed under or somehow through the doorway.
- Illumination: Lighting for CCTV functionality must remain sufficient relative to a variety of situations such as loss of commercial power, loss of interior natural/artificial light, and nighttime surveillance. Artificial and emergency lighting must be sufficient to support surveillance and playback particularly of high-risk areas.
- Maintenance: Optimal operations, including actual and recorded images, are achieved through regular testing and routine maintenance. Daily checks of camera views and weekly playback of recordings is required, and any identified deficiencies in the system shall be addressed as soon as possible.
- Housings: All cameras and associated cabling must be protected from tampering and vandalism. External cameras must be enclosed in tamper resistant housings.
- PTZ: In general, PTZ cameras should be used to augment fixed cameras, not replace them. Parking areas may be monitored by a combination of fixed and PTZ cameras.
- Identification: Combination intercom/camera devices must be used at entry points, particularly main entry and loading dock areas to aid in establishing identity prior to opening doors and permitting access.
- Camera Call-Up: Certain cameras such as PTZ cameras must be programmed and pre-positioned to support alarm call up in response to emergency exit doors and other critical entry/exit points such as those affiliated with the loading dock and to record such events.
- Continuous Recording: In general, these guidelines require continuous recording. However, configuration may include event recording features. Event recording is prompted by motion and/or IDS alarm activation particularly during times when the site is unattended or where surveillance involves spaces where little human activity takes place. Such a configuration may save space pertinent to recording video. Critical areas where incoming mail is opened must have continuous recording. Other high risk and low risk

areas can have motion activated or event recording provided that daily camera checks and weekly playback reviews are being performed.

- Access Control: System configuration may include integration with access control. For example, while attempting to use an expired badge to gain access, a pre-programmed CCTV camera will record the event (if not already in a continuous recording mode).and a guard will be alerted via monitor notification at the main guard station.

- Digital Recording: The contractor is required to provide and record surveillance of the mail processing area(s) using DVR/NVR systems, including the use of DVRs and if needed, appropriate video storage units. The DVR system must have duplex capabilities (the ability to play recorded video images while recording live images) and be supported by the necessary peripheral security equipment to ensure effectiveness and compatibility.

- Tampering: Recording and playback equipment must always be secured to prevent tampering and unauthorized use. Restricted access and usage must be managed by contractor's officials fully vetted under the IRS contract.

- Video Cassette Recording (VCR): VCR, technology and the use of VCR tapes are not acceptable due to disadvantages such as time-lapse recording.

- Virtual Real Time Recording: Recording must be conducted at a speed which will eliminate unwanted excessive stop action, or time lapse, which distracts from its usefulness including forensic value. System configuration and other factors related to digital technology may impact how well images are recorded; however, TIGTA has specified a minimum rate recording speed of 3.5 frames per second.

- Retention of Video Recordings: For PCA sites, video recordings of critical areas must be retained for one year. Other areas considered high risk must be retained for 6 months. Low risk areas must be retained for 30 days. For print vendors, high risk areas must be retained for 90 days, and low risk areas for 30 days. After the end of the retention period, image media may be destroyed or recorded over. If playback is stored on separate image media such as disks or supplemental hard drive, effective and appropriate safeguards must be in place to protect recorded images.

- Quality of Video Playback: Playback, of recorded video and the effectiveness and clarity of recorded images is critical to the design aspect of the CCTV system and is of paramount importance to the Government for reasons that support accountability, prudent practice, and forensic value. Consideration must be given to the overall CCTV design and system used, so factors that can degrade resolution or image quality (e.g., video compression, time lapse, recorder speed) will be minimized. Video must be able to be played back at or above the minimum recording speed of 3.5 frames per second.

- Internal or in-house playback reviews: On a weekly basis, the contractor must ensure CCTV playback is working as designed (functionality) by examining playback from at least 25% of the camera population and must be reviewed for at least one minute. Results from this review must be documented on a log.

- Weekly Video Playback Review Log must contain the following information; refer to Exhibit 6, Weekly Video Playback Review Log, for sample of log:

    - Review Date;
    - Review Name;
    - Recording Speed (if applicable);
    - DVR (if applicable) & associated camera;
    - Time/Date of video playback segment;
    - Clear Picture;
    - Imbedded date and time correct: y/n; and
    - Any other problems or concerns.

The new Network Video Recorders (NVR) utilize "cloud computing" where video is stored on several large computer hard drives and the recording speed cannot be determined and/or is not displayed. Also, because all the cameras are input into one centralized NVR and not a traditional 16 input DVR the specific NVR cannot be determined. Therefore, these 2 required items: recording speed & specific DVR should be removed from weekly video playback review log checklist.

- Documentation and Remediation: Acceptable measures must be put in place to channel and resolve problems related to playback. In addition, these measures must be documented as procedures in media such as post orders, standard operating procedures, and/or roles and responsibilities.

- Manual Camera Review: Daily, the contractor must manually scan through all cameras to ensure connectivity or a picture exists. This manual review is in addition to any automated or system capability designed to detect and report connectivity or communication problems. Results from this daily scan, including any significant findings, must be documented on a log.

    - In addition, reporting and remediation efforts to timely address problems associated with this daily scan must be in place and documented.

- Matrix: A document listing cameras and related accessories must be developed.

- CCTV Specifications: Upon request, the contractor must provide access to CCTV manufacture specifications on any and all CCTV related equipment and peripherals. These and other specifications, including as-built plans, diagrams, and schematics

provided by the CCTV design specialist or contractor must be maintained on-site and secured by a FA official.

Data Center Controls

The primary room must be a secured room/space 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 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 persons 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-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 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: New OMB & FAR Privacy Contract Requirements

OMB M-17-12

At a minimum, contracts should include terms that:

- Require the contractor to cooperate with and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach.
- Require contractors and subcontractors (at any tier) to properly encrypt PII in accordance with OMB Circular A-130 and other applicable policies and to comply with any agency-specific policies for protecting PII;
- Require regular training for contractors and subcontractors (at any tier) on how to identify and report a breach;
- Require contractors and subcontractors (at any tier) to report a suspected or confirmed breach in any medium or form, including paper, oral, and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy and US-CERT notification guidelines;
- Require contractors and subcontractors (at any tier) to maintain capabilities to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector;
- Allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with this Memorandum, the agency's breach response plan, and to assist with responding to a breach;
- Identify roles and responsibilities, in accordance with this Memorandum and the agency's breach response plan; and,
- Explain that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor (at any tier) failed to provide adequate safeguards.

Subpart 24.3 of the Federal Acquisition Regulations require

24.301 Privacy Training

(a) Contractors are responsible for ensuring that initial privacy training, and annual privacy training, thereafter, is completed by contractor employees who:

(1) Have access to a system of records;

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

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

(b) Privacy training shall address the key elements necessary for ensuring the safeguarding of personally identifiable information or a system of records. The training shall be role-based,

provide foundational as well as more advanced levels of training, and have measures in place to test the knowledge level of users. At a minimum, the privacy training shall cover–

(1) The provisions of the Privacy Act of 1974 (5 U.S.C. 552a), including penalties for violations of the Act;
(2) The appropriate handling and safeguarding of PII;
(3) The authorized and official use of a system of records or any other PII;
(4) The restriction on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise access PII;
(5) The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling, or use of PII; and
(6) Procedures to be followed in the event of a suspected or confirmed breach of a system of records or unauthorized disclosure, access, handling, or use of PII (see OMB guidance for Preparing for and Responding to a Breach of Personally Identifiable Information).

(c) The contractor may provide its own training or use the training of another agency unless the contracting agency specifies that only its agency-provided training is acceptable (see 24.302(b)).

(d) The contractor is required to maintain and, upon request, to provide documentation of completion of privacy training for all applicable employees.

(e) No contractor employee shall be permitted to have or retain access to a system of records, create, collect, use, process, store, maintain, disseminate, disclose, or dispose, or otherwise handle PII, or design, develop, maintain, or operate a system of records, unless the employee has completed privacy training that, at a minimum, addresses the elements in paragraph (b) of this section.

Appendix F: Reference

CIRCULAR NO. A-108 Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A108/omb_circular_a-108.pdf

CIRCULAR NO. A-130 Managing Information as a Strategic Resource
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

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 Acquisition Regulation Subpart 24.3—Privacy Training
https://www.acquisition.gov/far/current/html/Subpart%2024_3.html

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 Manuals 1.15, Records and Information Management series http://irm.web.irs.gov/Part1/Chapter11/Section1/IRM1.11.1.asp

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: https://www.irs.gov/irm/part10/irm_10-008-002r

Internal Revenue Manual 10.23.2, Contractor Investigations https://www.irs.gov/irm/part10/irm_10-023-002

OMB M–17–06 – Policies for Federal Agency Public Websites and Digital Services https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-06.pdf

OMB M–17–12 – Preparing for and Responding to a Breach of Personally Identifiable Information https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf

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 Rev. 5, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, refer to NIST Special Publication (SP) 800- 53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations

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 https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

Office of Management and Budget Memorandum 08-23:
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2008/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

Publication 4812 (Rev. 11-2021) Catalog Number 54170T Department of the Treasury **Internal Revenue Service** www.irs.gov