Enterprise Technology Strategy and Services Policy 10-11

Federal Tax Information Access

Brian Tardiff, CISO
doa.entsec@doit.ri.gov

1. Purpose

Establish policy that adequately protects and ensures the confidentiality of federal tax information (FTI) in accordance with Internal Revenue Service (IRS) has issued Publication 1075 entitled “Tax Information Security Guidelines for Federal, State, and Local Agencies” (IRS Publication 1075). Ensure that state agencies, as a condition of receiving FTI, maintain compliance with IRS Publication 1075.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

Federal Tax Information (FTI) Federal tax returns and return information (and information derived from it) in the state agency’s possession or control covered by confidentiality protections of the Internal Revenue Code (IRC) and subject to IRC 6103(p)(4) safeguarding requirements, including Internal Revenue Service (IRS) oversight. FTI includes return or return information received directly from IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or other entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement. FTI includes any information created by the recipient that is derived from federal return or return information received from IRS or obtained through a secondary source. Safeguarding FTI is critical to protecting taxpayer confidentiality as required by IRC 6103 and may not be masked to change the character of information to circumvent IRC 6103 confidentiality requirements.

1 State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State colleges, the General Treasurer, the Attorney General, or the Secretary of State.
Information Received from Taxpayers or Third Parties
Copies of tax returns or return information provided to the agency directly by the taxpayer or his/her representative (e.g. W-2’s, Form 1040, etc.) or obtained from public information files (e.g. federal tax lien on file with the county clerk, Offers in Compromise available for public inspection; court records, etc.) is not protected FTI that is subject to the safeguarding requirements of IRC 6103(p)(4). If the agency independently verifies FTI provided by the IRS or a secondary source with the taxpayer or a third-party source, the verified information is not FTI as long as the IRS source information is replaced or overwritten with the newly provided information.

Least Privilege
The principle that system users should be granted only the privileges required to perform their official duties and job functions.

Mobile Device
A computing device that is easily portable, has its own operating system, and is able to run application software. Typically, mobile devices have a display screen, a method to input data (e.g. touch screen, touch keyboard, miniature keyboard), and the ability to communicate and transfer data wirelessly (e.g. Wi-Fi, Bluetooth). Examples of mobile devices include, but are not limited to, tablets, laptops, notebooks, smartphones, and other portable computing devices.

Multifactor Authentication (MFA)
A method of authentication that requires at least two forms of independent credentials be verified prior to being granted access: something the user knows (e.g. password), something the user is (e.g. biometric), and/or something the user has (e.g. security token).

Need to Know
Limiting access to FTI to individuals with a need-to-know. Under need-to-know restrictions, even if an individual has the authority to access FTI, the individual would not be granted access to FTI unless it is necessary to perform his/her official duties with regard to the purpose for which the FTI will be used.

Personally Identifiable Information (PII)
Data, including FTI, that can be used either alone or in combination with other data to identify an individual. FTI may include the following PII elements (or any combination thereof):
- Name associated with the filing
- Mailing address, email address
- Identification number, telephone number, social security number, bank account number
- Place and date of birth
- Mother’s maiden name
- Biometric data (e.g. height, weight, eye color, fingerprints)
Return and Return Information
Any tax or information return, estimated tax declaration, or refund claim (including amendments, supplements, supporting schedules, attachments, or lists) required by or permitted under the IRC and filed with the IRS by, on behalf of, or with respect to any person or entity. Examples of returns include forms filed on paper or electronically (e.g. forms 1040, 941, 1120). Forms include supporting schedules, attachments, or lists that are supplemental to or part of such a return. For more information, see IRS Publication 1075 Section 1.4.2.

Security Control
A safeguard or countermeasure prescribed for an information system or an agency designed to protect the confidentiality, integrity (including non-repudiation and authenticity), and availability of its information that meets a set of defined security requirements. There are three (3) classes of security controls: Management, Operational, and Technical. Security controls need periodic assessment to provide the information necessary to determine the extent to which the controls are implemented correctly, if they’re operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

Separation of Duties
The principle that roles and responsibilities should be divided among different users so that no single individual may subvert the information system or a critical business function.

Unauthorized Access
Access to FTI is permitted only to individuals who require the FTI to perform their official duties and as authorized under the IRC. FTI must never be indiscriminately disseminated, even within the recipient agency, body, or commission. Agencies must evaluate the need for FTI before the data is requested or disseminated. For more information, see IRC 6103 and IRS Publication 1075 Section 1.4.5.

Unauthorized Disclosure
An unauthorized disclosure occurs when an entity or individual with authorization to receive FTI knowingly or with gross negligence discloses FTI to another entity or individual who does not have authority. Subject to the disclosure provisions of IRC 6103, agencies may need to disclose FTI to outside entities (e.g., for prosecution, appeals, or collection processes) as long as the receiving entity has a need-to-know and the individual recipient has authority under IRC 6103 to receive it. If the individual does not have a need-to-know, this constitutes an unauthorized disclosure. Additionally, an unauthorized disclosure has occurred when FTI is knowingly or, due to gross negligence, provided to an individual who does not have the statutory right to have access to it. Even without willfulness or gross negligence, FTI is not to be disclosed to entities or individuals who are not authorized by IRC 6103 to have it. For more information, see IRC 6103 and IRS Publication 1075 Section 1.4.6.

Virtual Desktop Infrastructure (VDI)
Virtualization technology that hosts a desktop operating system on a centralized server within a data center. VDI is a variation on the client-server computing model, sometimes referred to as server-based computing. Examples include VMWare and Citrix. VDI provides users access
Division of Information Technology

to enterprise resources, including a virtual desktop from locations both internal and external to the agency’s network. In a VDI environment, a user can access FTI by connecting to a virtual workstation via a vendor-specific agent, connection client, or through an internet browser from practically any mobile device with internet access.

4. Procedures for Compliance

4.1. IRS Publication 1075. IRS Publication 1075 provides federal, state, and local agencies with tax information security guidelines for safeguarding and protecting federal tax returns and returns information. Employees and third-party entities authorized to access FTI will maintain compliance with IRS publication 1075 guidelines.

4.2. Third-Party Contract Agreements. Contract agreements with vendors and third parties, as well as their subcontractors and subsidiaries, granted access to FTI will include appropriate IRS Publication 1075 language. Refer to IRS Publication 1075 Exhibit 7 for safeguarding FTI contract language.

4.3. Certification and Acceptance. Covered employees and third-party entities with access to FTI will certify, both prior to being granted access and annually thereafter, their acceptance and understanding of policies and procedures for safeguarding FTI by signing the “Certification and Acceptance” form located in Appendix A of this policy. The agency will maintain signed forms on file and send a copy of the signed form to the ETSS Enterprise Information Security Office (doa.entsec@doit.ri.gov).

4.4. Securing FTI.

4.4.1. Alternate Worksites. Controls used at alternate worksites that access, receive, store, process, or dispose of FTI will provide similar security as controls in place at primary worksites used for securing FTI including. Controls will employ appropriate encryption mechanisms in accordance with approved ETSS and IRS data encryption requirements (see ETSS Data Encryption Policy 05-03 and IRS Publication 1075 section 7.1.2). Portable removable media, including laptops, mobile devices, and paper, will be appropriately secured with a locking cable, inside a locked cabinet, locked office, behind a locked door, etc. Media containing FTI will be sanitized and destroyed in accordance with approved ETSS media sanitization methods (see ETSS Media Handling and Security Policy 05-01). The agency will perform and formally document annual inspections of alternate work sites to ensure that safeguards are adequate.

4.4.2. Access Restrictions. FTI will only be accessed or viewed by authorized individuals. FTI will not be accessed, received, stored, processed, or disposed by any covered individual, third party, or via information technology infrastructure that is located outside of the United States or its territories. MFA is required to access applications and systems that store FTI when traversing the public internet,
regardless of the transmission method. FTI will be clearly labeled “Federal Tax Information” and handled so it does not become misplaced or available to unauthorized personnel.

4.4.3. Restricted Area Access. A restricted area is an area where entry is limited to authorized personnel (individuals assigned to the area). All restricted areas will meet secured area criteria or provisions must be made to store FTI in appropriate containers during non-duty hours. Restricted areas will be prominently posted and separated from non-restricted areas by physical barriers that control access. Employee, vendor and non-agency personnel, and visitor access to restricted areas by will be controlled. Gaining access to a restricted area by “tailgating” or “piggybacking” is prohibited, regardless if the individual is authorized to enter the restricted area. All personnel must scan their ID badge when entering a restricted area. To facilitate the entry of personnel who have a frequent and continuing need to enter a restricted area, but are not assigned to the area, the agency will maintain an Authorized Access List (AAL) for agency employees and vendor/non-agency personnel so long as Minimum Protection Standards are maintained (see section 4.7.1 of this policy). The AAL will be updated monthly to reflect changes in access requirements. The AAL will include the following:

Agency Employee AAL
- Name of individual
- Agency or department name
- Name and phone number of agency POC
- Address of agency POC
- Purpose for access

Vendors and Non-Agency Personnel AAL
- Name of vendor/contractor/non-agency personnel
- Name and phone number of agency Point of Contact authorizing access
- Name and address of vendor POC
- Address of vendor/contractor
- Purpose and level of access

4.4.4. Visitor Access. The agency will maintain a restricted area visitor log at a designated entrance to the restricted area and all visitors (individuals not assigned to the area) entering the area shall be directed to the designated entrance. The visitor log will include the following information:
- Name and agency of the visitor
- Signature of visitor
- Form of identification
- Date of access
- Time of entry and departure
- Purpose of visit
- Name and agency of person visited
4.4.5. **Minimum Protection Standards (MPS).** The MPS or “two barrier” rule applies to FTI, beginning at the FTI itself and extending outward to individuals without a need-to-know. Protected information must be containerized in areas where non-authorized employees may have access after-hours. MPS is applied on a case-by-case basis to secure perimeters, secure rooms, secure employee access, and secure containers. See IRS Publication 1075 Table 3 (minimum protections standards) for more information.

4.4.6. **Storing Data.** FTI may be stored on hard disks only if agency-approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance including upgrades, and are being used. Access controls must include password security, an audit trail, encryption, virus detection, and data overwriting capabilities.

4.4.7. **Off-Site Storage.** Media containing FTI, which is sent to an off-site storage facility, will be properly secured, labeled, and protected from access by unauthorized individuals. The media may not be stored on open shelving, unless the shelving is in a restricted area accessible only to individuals with authorized access to FTI. Media containing FTI may not be released to a contractor operated off-site storage facility unless the media is encrypted and labeled as containing “federal tax information”, is locked in a secured container, and the agency retains the key to the secured container.

4.4.8. **Media and Devices.** Only state-owned devices are authorized to access, receive, process, or store FTI. Accessing FTI via non-state-owned or personal devices is strictly prohibited. Mobile devices and removeable media will be secured, as appropriate, with a locking cable, inside a locked cabinet, locked office, behind a locked door, etc. Removeable media containing FTI will be labeled as “federal tax information”. Only agency-approved security access control devices and agency-approved software will be used. Copies of illegal and non-approved software will not be used. Electronic media that is to be reused must have files overwritten or degaussed. Collaborative devices attached to computers with access to FTI will not be remotely activated and will employ alerts that notify the end user when the devices are activated. Multi-functional devices (any combination of printer, copier, scanner, fax) will require a user to authenticate to the device with a unique username and password, encrypt FTI going to or from the device, not fax or email FTI from the device, and not store FTI locally on the device.

4.4.9. **Email.** Email containing FTI will be encrypted using FIPS 140-2 validated encryption algorithms. Mail server and network equipment supporting email infrastructure will be hardened/patched against known vulnerabilities and protected against malware. Audit logs of email containing FTI will capture header, sender, recipient, date sent, and sender/recipient mail server information (name, IP address, transmission result, error codes). Email containing FTI will only be accessed from
Email containing FTI will be labeled to inform the recipient that it contains FTI. Prior to emailing FTI, senders will verify that only authorized individuals are in the email recipient list. Automatically forwarding emails containing FTI to other email addresses is strictly prohibited. FTI will only be sent via email attachments and not entered in the body of the email. End users will delete emails containing FTI from the mail client inbox when no longer needed. End users will log-off from workstations and never leave them unattended in a logged-on state.

4.4.10. Facsimile (Fax). Fax machines will be placed in secured areas. Trusted staff should be physically present at fax machines during transmissions of FTI. Broadcast lists and other preset numbers of frequent recipients of FTI will be maintained. Fax transmissions will include a cover sheet that provides recipients with explicit guidance, including a notification as to the sensitivity of the faxed data, the need for protection, and a notice to unintended recipients to contact the sender via telephone (collect call, if necessary) to report the disclosure of FTI and confirm the destruction of the information.

4.4.11. Paper. FTI printed from electronic to paper media or scanned from paper to electronic media will be tracked via logs. Paper documents containing FTI will be stored in controlled areas (e.g. restricted zones, secure rooms, locked rooms or cabinets) and monitored to detect and respond to unauthorized access. Paper documents containing FTI will be destroyed and disposed of by burning, mulching, pulping, shredding, or disintegrating.

4.5. Access Control

4.5.1. Access Control Policy and Procedures (AC-1). The agency will develop, document, disseminate, review, and annually update an access control policy and procedures.

4.5.2. Account Management (AC-2). The information system will automatically disable inactive accounts after 120 days of inactivity. The agency will:
- Identify information system account types that access FTI to support agency missions/business functions.
- Assign account managers for information system accounts.
- Establish conditions for group and role membership.
- Identify authorized users of the information system.
- Specify access privileges for each information system account.
- Require approval from authorized personnel for requests to create information system accounts. Privileged users require approval from the system owner.
- Create, enable, modify, disable, and remove information system accounts in accordance with documented agency account management procedures.
- Monitor the use of information system accounts.
• Notify account managers when accounts are no longer required, users have been terminated or transferred, or when information system usage or need-to-know requirements change.
• Authorizes access to information systems that receive, process, store, or transmit FTI based on a valid access authorization and need-to-know permissions required by the agency or associated missions/business functions.
• Annually reviews information system accounts for compliance with account management requirements.
• Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

4.5.3. Access Enforcement (AC-3). The information system will enforce (i) approved authorizations for logical access to information and system resources and (ii) a role-based access control policy over defined subjects and objects, and controls access to FTI based upon valid access authorizations, intended system usage, and the authority to be disclosed FTI.

4.5.4. Information Flow Enforcement (AC-4). The information system will enforce approved authorizations for controlling the flow of FTI within the system and between interconnected systems based on the technical safeguards in place to protect the FTI. For additional security and protection requirements, see IRS Publication 1075 section 9.4.3 (email communications), section 9.4.4 (fax equipment), and section 9.4.9 (multi-functional devices).

4.5.5. Separation of Duties (AC-5). The agency will separate the duties of individuals, document separation of duties of individuals, and define information system access authorizations to support separation of duties.

4.5.6. Least Privilege (AC-6). The information system will audit the execution of privileged functions and prevent non-privileged users from executing privileged functions (e.g. disabling, circumventing, or altering implemented security safeguards or countermeasures). The agency will (i) explicitly authorize access to FTI, (ii) employ the concept of least privilege for users authorized to access FTI, (iii) require that users of information system accounts with access to FTI use non-privileged accounts when accessing non-security functions, and (iv) restrict privileged accounts on the information system to a limited number of individuals with a need to perform administrative duties.

4.5.7. Unsuccessful Logon Attempts (AC-7). The information system will automatically lock user accounts after three (3) consecutive invalid logon attempts. The account will remain locked for a minimum of 15 minutes.

4.5.8. System Use Notification (AC-8). Prior to granting access to the system, the information system will display (i) an IRS-approved warning banner to users that provides privacy and security notices, (ii) state that the system contains U.S.
government information, (iii) state that user actions are monitored and audited, and (iv) state that unauthorized use of the system is prohibited and subject to criminal and civil sanctions.

For publicly accessible systems, the information system will (i) display an IRS-approved warning banner, (ii) display references to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities, and (iii) include a description of the authorized uses of the information system.

The warning banner will be retained on the screen until the user acknowledges the usage conditions and take explicit actions to logon or further access the information system. See IRS Publication 1075 exhibit 8 for sample IRS-approved warning banners.

4.5.9. Session Lock (AC-11). The information system will prevent further access to the system by initiating a session lock after fifteen (15) minutes of inactivity or upon receiving a user request. The session lock will remain in place until the user re-establishes access in accordance with approved identification and authentication procedures. Privileged accounts will only be unlocked by a system administrator.

4.5.10. Session Termination (AC-12). The information system will automatically terminate user-initiated sessions after thirty (30) minutes of inactivity. User-initiated sessions are different from network communications sessions, which address the termination of network connections (network disconnect) associated with communications sessions (see section SC-10 in this policy).

4.5.11. Permitted Actions without Identification or Authentication (AC-14). FTI may not be disclosed to individuals on the information system without proper identification and authentication. The agency will (i) identify specific user actions that can be performed on the information system without identification or authentication (consistent with agency mission/business functions), and (ii) document and provide supporting rationale in the Safeguard Security Report (SSR) for the information system the user actions not requiring identification and authentication.

4.5.12. Remote Access (AC-17). The agency will (i) establish and document usage restrictions, configuration and connection requirements, and implementation guidance for each type of remote access allowed and (ii) authorize the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs only. The information system will be configured to (i) monitor and control remote access methods, (ii) implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions, and (iii) route all remote accesses through a limited number of managed network access control points. Any remote access where FTI is accessed
Division of Information Technology

over a remote connection must be performed using MFA. FTI will not be remotely accessed from outside of the United States. See ETSS Policy 04-01 (virtual private network access) for more information.

4.5.13. Wireless Access (AC-18). The agency will (i) establish usage restrictions, configuration and connection requirements, and implementation guidance for wireless access, (ii) authorize wireless access to the information system prior to allowing such connections, and (iii) employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system. The information system will be configured to protect wireless access to the system using authentication and encryption. See ETSS Wireless Access Policy 04-02 and IRS Publication 1075 section 9.4.18 (wireless networks) for more information on protecting FTI on wireless networks.

4.5.14. Access Control for Mobile Devices (AC-19). The agency will (i) establish usage restrictions, configuration and connection requirements for agency controlled mobile devices, (ii) authorize connection of mobile devices to agency information systems, and (iii) employ encryption to protect the integrity and confidentiality of information on mobile devices. With the exception of laptops, mobile devices will be purged/wiped after ten (10) consecutive unsuccessful logon attempts. See ETSS Mobile Device Security Policy 10-04 for more information and mobile device requirements.

4.5.15. Use of External Information Systems (AC-20). External information systems and non-agency-owned equipment include any technology used to receive, process, transmit, or store FTI that is not owned and managed by the state. Unless approved by the IRS Office of Safeguards, the agency will prohibit (i) access to FTI from external information systems, other than through VDI, (ii) the use of agency controlled portable storage devices (e.g. flash drives, external hard drives) containing FTI on external information systems, and (iii) the use of non-agency-owned information systems, system components, or devices to process, store, or transmit FTI.

The agency will notify the Office of Safeguards 45 days prior to implementation of any non-agency-owned information system. The agency may allow the use of personally owned devices, without notification, only for the following purposes:

- A Bring Your Own Device (BYOD) is used to access email, where all requirements for mobile devices are met. A BYOD is a personally owned device (not owned by the agency) and is subset of external information systems. See IRS Publication 1075 section 9.4.8 (mobile devices) for more information.
- Remote access through a VDI environment, where all requirements for VDI are met. See IRS Publication 1075 section 9.4.13 (virtual desktop infrastructure) for more information.
4.5.16. **Information Sharing (AC-21).** The agency will restrict the sharing or re-disclosure of FTI only to authorized individuals and as approved by the IRS Office of Safeguards.

4.5.17. **Publicly Accessible Content (AC-22).** The agency will (i) designate and train individuals authorized to post information onto publicly accessible information systems, (ii) review the information prior to posting onto publicly accessible information systems to ensure FTI is not included, and (iii) perform quarterly reviews of the information posted on publicly accessible information systems for FTI and, if discovered, remove such information.

4.6. **Security Awareness and Training**

4.6.1. **Security Awareness and Training Policy and Procedures (AT-1).** The agency will develop, document, disseminate, review, and annually update a security awareness and training policy and procedures.

4.6.2. **Training Types.** A comprehensive training program is necessary to ensure the protection of FTI. Users should receive training, as appropriate, in accordance with their assigned roles, job duties, and functions. See IRS Publication 1075 section 6.2 (training requirements) for more information.

**Security Awareness Training (AT-2)**

Security awareness training provides basic security awareness training to information system users. All information system users, including contractors, will receive security awareness training as part of initial training for new users, when required due to information system changes, and annually thereafter.

**Disclosure Awareness Training (AT-2)**

Disclosure awareness training is specific to the protection of FTI and prevention of unauthorized disclosure. The agency will provide disclosure awareness training and recertification on an annual basis to all information system users, including contractors, needing to maintain their authorization to access FTI.

**Role-Based Training (AT-3)**

Role-based training provides individualized training customized to specific security roles and responsibilities. The agency will provide role-based training to personnel assigned security roles and responsibilities prior to granting access to the information system or performing assigned duties that require access to FTI, when required due to information system changes, and annually thereafter. Personnel with security roles and responsibilities include, but are not limited to, security officers/managers, network/system/database administrators, security specialists, programmer/system analysts, system owners, developers, and helpdesk.
Contingency Training
Contingency training provides individualized training to support backup and recovery requirements. The agency will provide contingency training to personnel assigned roles and responsibilities as they relate to the recovery of backup copies of FTI on an annual basis. This training may be included with role-based training, as appropriate.

Incident Response Training
Incident response training provides personnel with requirements and procedures for reporting unauthorized disclosures or data breaches of FTI. The agency will provide incident response personnel with agency-specific procedures for handling incidents. Incident response training will include IRS-specific requirements pertaining to incidents involving FTI.

4.6.3. Security Training Records (AT-4). The agency will document and monitor security training activities, including basic security awareness training and specific information system security training, and retain training records for five (5) years.

4.7. Audit and Accountability

4.7.1. Audit and Accountability Policy and Procedures (AU-1). The agency will develop, document, disseminate, review, and annually update an audit and accountability policy and procedures.

4.7.2. Audit Events (AU-2). An event is any observable occurrence in the information system. Security-relevant events enable the detection of unauthorized access to FTI data. Auditing must be enabled to the greatest extent necessary to capture access, modification, deletion, and movement of FTI by each unique user. The agency will review and update the list of events chosen to be audited on an annual basis and determine that the information system is configured to audit, at a minimum, the following events:
- All successful and unsuccessful logons and logoffs
- All system startups and shutdowns
- All actions, connections, and requests by privileged users and functions, such as:
  - System administrator commands
  - Changes to system settings
  - Switching accounts or running privileged actions from another account (e.g. Linux/Unix SU or Windows RUNAS)
- All creation, modifications, or deletions of objects, files, directories, accounts, groups, privileges, such as:
  - Password changes
  - Changes to user/groups/privileges
  - Changes to audit log files, including the clearing of audit log files
  - Start-up and shutdown of audit functions
  - Changes to applications and databases via batch files
Changes to application and database records, where the application has been bypassed to produce the change (e.g. via a file or other database utility)

- Changes to application-critical records
  - All successful and unsuccessful remote access attempts to information systems from outside of the state network (e.g. VPN, modems, dial-in access)
  - All system and data interactions regarding FTI

4.7.3. Content of Audit Records (AU-3). Audit record contents should include any information deemed critical to reconstructing the chronological order of activities leading to the event (e.g. software, hardware, process, filename). The information system will be capable of generating audit records containing details to facilitate the reconstruction of events. Audit record content will include:
  - Timestamp user logged in (date/time)
  - Identity of user generating event (user ID)
  - Event outcome (success/failure)
  - Event type/description
  - Event source/destination (IP address)
  - Timestamp event occurred (date/time)

4.7.4. Audit Storage Capacity (AU-4). The agency will allocate audit record storage capacity necessary to retain audit records for the required retention period of seven (7) years.

4.7.5. Response to Audit Processing Failures (AU-5). Audit processing failures include, but are not limited to, system and hardware errors, failures of audit record capturing mechanisms, and reaching the audit storage capacity limit. The information system will:
  - Monitor system operational status using operating system or system audit logs and verify functions and performance of the system. Logs shall identify where system process failures have occurred.
  - Provide a warning when audit record storage capacity utilization reaches 75%, 90%, and 100%. The information system will overwrite the oldest audit records or shut down, as appropriate, when maximum audit record storage capacity is reached.
  - Automatically alert system administrators and other designated personnel in the event of an audit processing failure.

4.7.6. Audit Review, Analysis, and Reporting (AU-6). The agency should identify events that may indicate potential unauthorized access or disclosure of FTI. For more information regarding proactive methods to detect unauthorized access to FTI, see IRS Publication 1075 table 10 (proactive auditing methods to detect unauthorized access to FTI). The agency will (i) review and analyze information system audit records weekly for indications of potential unauthorized access or disclosure of FTI and (ii) report findings in accordance with ETSS Guideline 10-12G (Incident Response Plan). If a finding involves potential unauthorized
disclosure of FTI, please report the finding in accordance with the “FTI Reporting Procedure” in section 4.4 of this policy. See IRS Publication 1075 section 10.0 (reporting improper inspections or disclosures) for more information.

4.7.7. Audit Reduction and Report Generation (AU-7). Audit reduction is a process that manipulates collected audit information and organizes this information in a summary format that is more meaningful to analysts. Audit reduction capability can include modern data mining techniques with advanced filters to identify anomalous behavior in audit records. The information system will provide an audit reduction and report generation capability that (i) supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents and (ii) does not alter the content or time ordering of audit records.

4.7.8. Time Stamps (AU-8). The information system will (i) use internal system clocks to generate audit record time stamps, (ii) record time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), and (iii) synchronize internal system clocks to an enterprise time source.

4.7.9. Protection of Audit Information (AU-9). The information system will protect audit information and audit tools from unauthorized modification, access, or destruction. The agency will authorize access to manage audit functionality only to security administrators or other designated security personnel (staff other than the system and network administrators). System and network administrators will not have the ability to modify or delete log entries. To ensure the protection of audit information, audit records should be backed up nightly to a system other than the audited system and cryptographic mechanisms should be implemented to protect the integrity of audit information and audit tools.

4.7.10. Audit Record Retention (AU-11). The agency will retain audit records for events identified in section 4.10.2 (AU-2) of this policy for a period of seven (7) years.

4.7.11. Audit Generation (AU-12). Audit records should be generated for any system used in the processing, transferring, or storing of FTI, including end-user environments (e.g. desktops, laptops), servers (e.g. file, print, web, firewalls, terminal servers), and network components (e.g. switches, routers, wireless). The information system will (i) provide an audit record generation capability for events defined in section 4.10.2 (AU-2) of this policy and (ii) generate audit records for the events with content defined in section 4.10.3 (AU-3) of this policy.

4.7.12. Cross-Agency Auditing (AU-16). For outsourced data centers and cloud providers, the agency will employ mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across agency boundaries. See IRS Publication 1075 section 5.4 (controls over processing) and section 9.4.1 (cloud computing environments) for more information.
4.8. **Security Assessment and Authorization**

4.8.1. **Security Assessment and Authorization Policy and Procedures (CA-1).** The agency will develop, document, dissemnate, review, and annually update a security assessment and authorization policy and procedures.

4.8.2. **Security Assessments (CA-2).** The agency will (i) develop a security assessment plan that describes the scope of the assessment, security controls and control enhancements, assessment procedures, assessment environment, assessment team, and assessment roles and responsibilities, (ii) assess the security controls in the information system and its environment on an annual basis to determine if the controls are implemented correctly, operating as intended, and producing the desired outcome to meet security requirement, (iii) produce a security assessment report that documents the results of the assessment, and (iv) provide results of the security control assessment to the agency’s authorizing official. An authorizing official is a senior level official at the agency with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency and enterprise operations, assets, and personnel.

4.8.3. **System Interconnections (CA-3).** The agency will (i) authorize connections from the information system to other information systems via Interconnection Security Agreements (ISA) or similar agreements, (ii) document interface characteristics, security requirements, duration, point of contact, associated risks, party accepting risks, and the nature of the information communicated for each interconnection, (iii) annually review and update, as required, the system interconnection, and (iv) employ deny-all and allow-by-exception policy for allowing systems that receive, process, store, or transmit FTI to connect to external information systems.

System interconnections should be terminated when the business case no longer requires the system interconnection or the authority to operate an interconnected system, ISA, or other similar agreement expires or is withdrawn. Upon terminating a system interconnection, relevant security controls should be re-assessed and appropriate security documentation (e.g. Risk Assessments, Contingency Plans, System Security Plans, Incident Response Plans) should be updated.

4.8.4. **Plan of Action and Milestones (CA-5).** The agency will develop a Plan of Action and Milestones (POA&M) for the information system and update the POA&M, as required, on a quarterly basis. A POA&M documents planned remedial actions to correct weaknesses or deficiencies noted during an assessment of security controls to reduce or eliminate known vulnerabilities in the information system. A POA&M allows the agency to track vulnerabilities identified by security controls assessments, security impact analysis, continuous monitoring activities, self-assessments, internal inspections, external audits, and any other vulnerabilities identified for information systems that receive, process, store, or transmit FTI. See
Division of Information Technology

IRS Publication 1075 section 6.5 (plan of action and milestones) for more information.

4.8.5. Security Authorization (CA-6). A security authorization is the permission granted by senior management to access an information system that is based on authorization decision documents to accept the risk to agency and enterprise operations, assets, individuals, other organizations. The agency will (i) assign an authorizing official (e.g. senior-level executive or manager) for the information system, (ii) ensure authorization is granted prior for information system processing prior to commencing operations, and (iii) update the security authorization every three (3) years or whenever there is a significant change to the information system.

4.8.6. Continuous Monitoring (CA-7). The strategy for implementing a continuous monitoring program should identify the security controls to be monitored, monitoring frequency, type of assessment, correlation and analysis, response activities, and responsibilities of personnel with continuous monitoring roles. The agency will develop and implement a continuous monitoring program that includes (i) agency-defined metrics that are monitored on an annual basis, and (ii) ongoing security control assessments and status monitoring of agency-defined metrics in accordance with the continuous monitoring strategy.

4.9. Configuration Management

4.9.1. Configuration Management Policy and Procedure (CM-1). The agency will develop, document, disseminate, review, and annually update a configuration management policy and procedures.

4.9.2. Baseline Configuration (CM-2). A baseline configuration is the technical, functional, and physical specifications that reflect the current information system architecture including, for example, standard software installed on workstations, laptops, servers, network components, and mobile devices, operating system and application versions and patch sets, configuration settings, network topology, and logical placement of system components within the system architecture. The agency will (i) develop and document the current baseline configuration of the information system, and (ii) review and update the baseline configuration annually and when required due to system upgrades, patches, or upon installation/upgrade of information system components.

4.9.3. Configuration Change Control (CM-3). Configuration change control for agency information systems comprises the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system modifications and upgrades, changes to baseline configurations, changes to configuration settings, unscheduled changes, and changes to remediate vulnerabilities. The agency will (i) identify the types of changes to be placed under configuration control, (ii) review and coordinate proposed configuration-controlled
changes to information systems via the ETSS Change Approval Board (CAB), (iii) test, validate, and document changes prior to implementing operating system changes, (iv) retain records of configuration-controlled changes for the life of the information system, and (v) audit and review activities associated with changes to the information system.

4.9.4. **Security Impact Analysis (CM-4).** The agency will perform an analysis of a proposed change to determine the potential impact to system security prior to the implementation of the proposed change. The security impact analysis should (i) be performed by appropriate agency personnel (e.g. system administrators, agency security managers, system engineers), (ii) include activities such as the review of security plans, conducting risk assessments, and performing tests within a test environment, and (ii) be scaled in accordance with the security category of the information system.

4.9.5. **Access Restrictions for Change (CM-5).** The information system owner will define, document, approve, and enforce physical and logical access restrictions associated with information system changes. The system owner should identify individuals authorized to perform configuration changes within the Configuration Management Plan (CMP) and document and maintain physical and logical access control lists of individuals authorized to make changes to an information system. Only authorized and qualified individuals may access the information system or its components for the purpose of initiating a change.

4.9.6. **Configuration Settings (CM-6).** Configuration settings are parameters within information system hardware, software, or firmware components that can be changed and, consequently, have an affect the security posture or functionality of the system. The agency will establish, document, implement, and monitor configuration settings for information system products that receive, process, store, or transmit FTI. Configuration settings should be in the most restrictive mode consistent with agency operational requirements. See IRS Publication 1075 section 9.3.5.6 (configuration settings) and the NIST Checklist Program Repository (https://nvd.nist.gov/ncp/repository), which is the authoritative source for platform checklists used by the IRS Office of Safeguards, for more information.

4.9.7. **Least Functionality (CM-7).** The agency will (i) configure the information system to provide only essential capabilities, (ii) prohibit or restrict the use of functions, ports, protocols, and services defined in IRS Office of Safeguards-approved compliance requirements, and (iii) review vulnerability assessments to identify functions, ports, protocols, and services deemed unnecessary or unsecure.

4.9.8. **Information System Component Inventory (CM-8).** The agency will document and maintain an inventory of information system components that (i) accurately reflects the current information, includes all components that store, process, or transmit FTI, and contains information that is sufficiently granular for component
tracking and reporting purposes, and (ii) is reviewed and updated annually (via manual or automated inventory checks) and as part of integral part of component installations, removals, and information system updates. The inventory should contain all necessary system component and software information, including hardware specifications (e.g. manufacturer, model, serial number, physical location, system owner), software platforms and applications (e.g. software version and license information), and networked components (e.g. machine names and network addresses). See IRS Publication 1075 (system component inventory) for more information.

4.9.9. **Configuration Management Plan (CM-9).** The agency will document, maintain, and implement a Configuration Management Plan (CMP) for the information system that (i) addresses roles, responsibilities, and configuration management processes and procedures, (ii) establishes processes and procedures for identifying configuration items throughout the system development life cycle (SDLC), (iii) defines information system configuration items and the items under configuration management, (iv) protects the CMP from unauthorized disclosure and modification, and (v) is reviewed annually and updated as required. A CMP defines system level processes and procedures for how configuration management will be implemented to support SDLC activities and should describe how (i) to move a change through the change management process, (ii) configuration settings and configuration baselines are updated, (iii) the information system component inventory is maintained, (iv) development, test, and operational environments are controlled, and (v) documents are developed, released, and, updated.

4.9.10. **Software Usage Restrictions (CM-10).** The agency will (i) authorize and approve software prior to it being installed, (ii) use and track software in accordance with licensing, contract agreements, and copyright laws, and (iii) control and document the use of authorized peer-to-peer file sharing technology to ensure it is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

4.9.11. **User-Installed Software (CM-11).** The agency will (i) adhere to established ETSS policies and standards governing software approved for installation, (ii) enforce software installation policies (if possible, via automated methods), and (iii) continuously monitor information systems for compliance.

4.10. **Contingency Planning**

4.10.1. **Contingency Planning Policy and Procedures (CP-1).** The agency will develop, document, disseminate, review, and annually update a contingency planning policy and procedures.

4.10.2. **Contingency Plan (CP-2).** The agency will (i) develop a contingency plan for the information system as part of an overall program for achieving continuity of
operations of its mission and business functions, (ii) review and update the contingency plan annually and after a change to the agency, information system, operational environment, or any problem arising from contingency planning testing or execution, (iii) distribute the contingency plan to key contingency personnel (individuals assigned contingency roles and responsibilities) initially and after an update, (iii) coordinate contingency planning activities with incident handling activities, and (iv) protect the contingency plan from unauthorized disclosure or modification. Contingency plans should:

- Identify essential mission/business functions and associated contingency requirements.
- Provide recovery objectives, restoration priorities, and associated metrics.
- Define contingency roles, responsibilities, and individuals assigned to contingency roles, including contact information.
- Address maintaining essential mission and business functions despite an information system disruption, compromise, or failure.
- Address information system restoration without weakening planned/existing safeguards.
- Be reviewed and approved by appropriate personnel, including the information system owner, data owner, business process owner, CIO, and CISO.

4.10.3. Contingency Training (CP-3). The agency will provide contingency training to all personnel assigned contingency roles and responsibilities within 3 months of being assigned a contingency role, annually thereafter as refresher training, and whenever the information system undergoes a significant change.

4.10.4. Contingency Plan Testing (CP-4). The agency will test the contingency plan annually based on the continuity requirements of the plan to determine its effectiveness and agency readiness to execute the plan, review the results of contingency plan tests, and, if necessary, initiate corrective actions. Contingency tests include walk-throughs, tabletop exercises, checklists, simulations, and comprehensive exercises.

4.10.5. Alternate Storage Site (CP-6). The agency will (i) establish an alternate storage site, including necessary agreements to permit the storage and retrieval of information system backup information and (ii) ensure that the alternate storage site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103. An alternate storage site is geographically distinct from a primary storage site and maintains duplicate copies of information and data. Alternate storage site agreements should specify access rules, physical and environmental conditions and protection requirements, and coordination of delivery/retrieval of backup media.

4.10.6. Alternate Processing Site (CP-7). The agency will (i) establish an alternate processing site, including necessary agreements to permit the transfer and
Division of Information Technology

resumption of information system operations, (ii) ensure equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within 12 hours for transfer/resumption, and (iii) ensure information security safeguards at the alternate storage site meet minimum protection standards and the disclosure provisions of IRC 6103. Alternate processing sites reflect requirements identified in the contingency plan to ensure that essential mission and business functions are reconstituted after a disruption, compromise, or failure. Alternate processing site agreements should identify physical and environmental protection requirements, access rules, and coordination of delivery and retrieval of backup media.

4.10.7. Information System Backup (CP-9). The agency will (i) perform backups of user-level and system-level information, as well as information system and security-related documentation, at least weekly and (ii) protect the confidentiality of backup information at storage locations. Backups should be tested monthly (e.g. random file testing) to ensure media reliability and information integrity.

4.10.8. Information System Recovery and Reconstitution (CP-10). The agency will provide for and ensure the information system can be recovered and reconstituted to a known state after a disruption, compromise, or failure.

4.11. Identification and Authentication

4.11.1. Identification and Authentication Policy and Procedures (IA-1). The agency will develop, document, disseminate, review, and annually update an identification and authentication policy and procedures.

4.11.2. Identification and Authentication (Agency users) (IA-2). The information system will (i) uniquely identify and authenticate agency users (or processes acting on behalf of agency users), (ii) implement MFA for all remote network access to privileged and non-privileged accounts for information systems that receive, process, store, or transmit FTI, and (iii) ensure that on factor in the MFA process uses a separate device from the system gaining access. Implement multi-factor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. See NIST 800-63 (digital identity guidelines) for more information.

4.11.3. Device Identification and Authentication (IA-3). The information system will uniquely identify and authenticate devices before establishing a connection (e.g. MAC address, IP address, Radius, Kerberos, etc.).

4.11.4. Identifier Management (IA-4). The agency will manage information system identifiers by (i) receiving authorization from designated personnel to assign an individual, group, role, or device identifier, (ii) selecting and assigning an identifier
Division of Information Technology

to the intended individual, group, role, or device, (iii) preventing reuse of identifiers for a minimum of one year, and (iv) disabling identifiers after 30 days of inactivity.

4.11.5. Authentication Management (IA-5). The agency will manage information system authenticators by:

- Verifying the identity of the individual, group, role, or device receiving the authenticator.
- Establishing initial authenticator content for authenticators defined by the agency.
- Ensuring authenticators have sufficient strength or their intended use.
- Establishing procedures for (i) initial authenticator distribution, (ii) lost, compromised, or damaged authenticators, and (iii) revoking authenticators.
- Changing authenticator default content prior to information system installation.
- Establishing authenticator lifetime restrictions and reuse conditions.
- Changing or refreshing authenticators periodically, as required, based on type.
- Protecting authenticator content from unauthorized disclosure and modification.
- Requiring individuals take specific security safeguards to protect authenticators.
- Changing authenticators for group/role accounts when group/role membership changed.
- For password-based authentication requirements, see ETSS Enterprise Password Security Policy 10-01.

4.11.6. Authenticator Feedback (IA-6). The information system will obscure feedback of authentication information during the authentication process and does not provide information that would allow unauthorized individuals to compromise authentication mechanisms.

4.11.7. Cryptographic Module Authentication (IA-7). The information system will implement mechanisms for authentication to a cryptographic module that meets the requirements of applicable mandates and guidance for such authentication. All FTI electronic transmissions will be encrypted using FIPS 140-2 validated cryptographic modules. Only modules tested and validated by NIST to FIPS 140-2 standards meet the applicability requirements for cryptographic modules to protect sensitive information (see list of validated cryptographic modules at http://csrc.nist.gov/).

4.11.8. Identification and Authentication (Non-Agency Users) (IA-8). The information system will uniquely identify and authenticate non-agency users (or processes acting on behalf of non-agency users).

4.12. Incident Response

4.12.1. Incident Response Policy and Procedures (IR-1). The agency will develop, document, disseminate, review, and annually update an incident response policy and procedures.
4.12.2. Incident Response Training (IR-2). The agency will provide incident response training to all information system users consistent with assigned roles and responsibilities prior to assigning an incident response role or responsibility, when required after an information system change, and annually thereafter. A training log will be maintained that includes participant names, information system names, type of training, and date of training.

4.12.3. Incident Response Testing (IR-3). The agency (i) will perform annual tabletop exercises using scenarios that include breach of FTI to test the ability of the agency to respond to FTI incidents and (ii) document and review an after-action report to improve existing processes, policies, and procedures. See IRS Publication 1075 section 10.3 (incident response procedures), NIST SP 800-84 (guide to test, training, and exercise programs), and NIST SP 800-115 (guide to information security testing) for more information.

4.12.4. Incident Handling (IR-4). The agency will (i) implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery, (ii) coordinate incident handling activities with contingency planning activities, (iii) incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and (iv) implement the resulting changes accordingly. An effective incident handling capability includes coordination among agency entities (e.g. mission/business owners, information system owners, authorizing officials, human resources personnel, physical and personnel security offices, legal departments, operations personnel).

4.12.5. Incident Monitoring (IR-5). The agency will track and document security incidents potentially affecting the confidentiality of FTI.

4.12.6. Incident Reporting (IR-6). The agency will require personnel to report suspected security incidents to internal agency incident response resources upon discovery of the incident. If the agency experiences or suspects a breach or loss of PII or security incident that involves FTI, including unauthorized disclosure or access to FTI, the agency will immediately, but no later than 24 hours after identifying a possible issue involving FTI, notify the ETSS CISO, contact the special agent-in-charge, contact the Treasury Inspector General for Tax Administration (TIGTA) of the New York field office at (917)-408-5640, and email the IRS Office of Safeguards at safeguardreports@irs.gov. When emailing the Office of Safeguards, please include the following information in the data incident report (do not include any FTI):

- Name of agency and agency Point of Contact.
- Date and time incident occurred.
- Date and time incident were discovered.
- How incident was discovered.
- Description of incident and data involved, including specific data elements (if known).
• Physical address where incident occurred and IT equipment involved (e.g. laptop, server, mainframe).

Immediate notification to the IRS Office of Safeguards is the most important factor, not the completeness of the data incident report. Send the data incident report electronically and encrypted via an IRS-approved encryption technique. Use the term “Data Incident Report” in the subject line of the email.

4.12.7. Incident Response Assistance (IR-7). The agency will provide an incident response support resource, integral to the agency incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

4.12.8. Incident Response Plan (IR-8). The agency will develop an incident response plan that:
• Describes the structure of and roadmap for implementing the incident response capability.
• Meets unique agency requirements (e.g. mission, size, structure, functions).
• Defines reportable incidents.
• Provides metrics for measuring the incident response capability at the agency.
• Defines resources and management support necessary to maintain an effective incident response capability.
• Is reviewed and approved by designated agency officials.

The incident response plan will be (i) protected from unauthorized disclosure or modification, (ii) distributed to authorized incident response personnel, (iii) reviewed annually and updated, as required, to address changes to the information system, agency, or issues encountered during plan implementation, execution, or testing, and (iv) communicated to authorized incident response personnel within 30 days of a change being made to the incident response plan.

4.12.9. Information Spillage Response (IR-9). Information spillage refers to instances where sensitive information is inadvertently placed on information systems that are not authorized to process such information. The agency will respond to information spills by (i) identifying the specific information involved in the information system contamination, (ii) alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill, (iii) isolating the contaminated information system and eradicating the information from it, and (iv) identifying other information systems that may have been subsequently contaminated.
4.13. System Maintenance

4.13.1. System Maintenance Policy and Procedures (MA-1). The agency will develop, document, disseminate, review, and annually update a system maintenance policy and procedures.

4.13.2. Controlled Maintenance (MA-2). The agency will (i) schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and agency requirements, (ii) monitor and approve all maintenance activities, regardless whether performed on site or remotely, (iii) require explicit approval from an authorized individual at the agency to remove the information system or system component from agency premises for off-site maintenance, (iv) sanitize equipment to remove FTI from associated media prior to removal from agency premises for off-site maintenance, and (v) check all potentially impacted security controls to verify they’re still functioning properly following maintenance actions. Maintenance addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component, including scanners, copiers, and printers, conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). Maintenance records should include appropriate information, such as date and time of maintenance, name of individual/group performing maintenance, name of escort (if applicable), name and ID of information system or system component being maintained, and description of the maintenance performed.

4.13.3. Maintenance Tools (MA-3). The agency will approve, control, and monitor information system maintenance tools (e.g. hardware, software, firmware, packet sniffers, diagnostic test equipment) used for diagnostic and repair actions on agency information systems.

4.13.4. Non-Local Maintenance (MA-4). Nonlocal maintenance and diagnostic activities are activities performed by individuals communicating via an internal or external network. The agency will (i) approve, monitor, and maintain records of non-local maintenance and diagnostic activities, (ii) document policies and procedures for the establishment and use of non-local maintenance and diagnostic connections, (iii) allow the use of non-local maintenance and diagnostic tools only as consistent with agency policy and information system security plan, (iv) employ MFA for the establishment of non-local maintenance and diagnostic sessions, and (v) terminate sessions and network connections when non-local maintenance is completed.

4.13.5. Maintenance Personnel (MA-5). The agency will (i) establish a process for the authorization of maintenance personnel, (ii) maintain a list of authorized personnel, (iii) ensure non-escorted personnel performing maintenance have required access authorizations, and (iii) designate agency personnel with access authorizations and
technical competence to supervise maintenance activities of personnel who do not have required access authorizations.

4.14. Media Protection


4.14.2. Media Access (MP-2). Information system media includes both digital and non-digital media. The agency will restrict access to digital and non-digital media containing FTI to authorized individuals.

4.14.3. Media Marking (MP-3). The agency will label information system media containing FTI to indicate media distribution limits and other important handling information. Removeable media (e.g. CDs, DVDs, diskettes, magnetic tapes, external hard drives, flash drives) and information system output containing FTI (reports, documents, data files, back-up tapes) will be labeled indicating “Federal Tax Information”.

4.14.4. Media Storage (MP-4). The agency will (i) physically control and securely store media containing FTI and (ii) protect information system media until the media is destroyed or sanitized. Security may be provided for a document, item, or area in various ways including, but are not limited to, locked containers of various types, vaults, locked rooms, locked rooms that have reinforced perimeters, locked buildings, guards, electronic security systems, fences, identification systems, and control measures. See IRS Publication 1075 section 4.0 (secure storage) for more information.

4.14.5. Media Transport (MP-5). The agency will (i) protect, control, and maintain accountability of digital and non-digital media during transport outside of controlled areas, (ii) document and track activities associated with the transport of information system media to ensure FTI reaches its intended destination, and (iii) restrict the activities associated with the transport of information system media to authorized personnel. The information system will implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. See IRS Publication 1075 section 4.4 (FTI in transit) for more information.

4.14.6. Media Sanitization (MP-6). The agency will (i) sanitize media containing FTI prior to disposal, release out of agency control, or release for reuse, (ii) employ sanitization mechanisms that are commensurate with the security category or classification of the information, and (iii) review, approve, track, document, and verify media sanitization and disposal actions. FTI will be sanitized in accordance with federal and ETSS-approved sanitization requirements. If media will be reused
by the agency for storing FTI and not leave agency control, FTI will be cleared from the media. If media will be reused for non-FTI functions or will be leaving agency control, FTI will be purged from the media. If the media will not be reused at all, the media will be destroyed. See ETSS Media Handling and Security Policy 05-01, ETSS Media Sanitization Guideline 05-01G, and IRS Publication 1075 section 9.4.7 (media sanitization) for more information.

4.15. Physical and Environmental Protection

4.15.1. Physical and Environmental Protection Policy and Procedures (PE-1). The agency will develop, document, disseminate, review, and annually update a physical and environmental protection policy and procedures.

4.15.2. Physical Access Authorizations (PE-2). The agency will (i) develop, approve, maintain, and periodically review an Authorized Access List (AAL) of individuals authorized to access the facility where the information system resides, (ii) issue authorization credentials (e.g. ID badge) for facility access, (iii) promptly remove individuals from the AAL when access is no longer required, and (iv) enforce physical access authorizations to the information system in addition to the physical access controls for the facility at spaces where FTI is received, processed, stored, or transmitted.

4.15.3. Physical Access Control (PE-3). The agency will:
   • Enforce physical access authorizations at entry and exit points to facilities where information systems that receive, process, store, or transmit FTI reside by (i) verifying individual access authorizations before granting access to the facility and (ii) controlling ingress and egress to the facility using physical access control systems/devices or security guards.
   • Maintain physical access audit logs for entry/exit points.
   • Provide security safeguards to control access to areas within the facility officially designated as publicly accessible (e.g. cameras, security guards, card readers).
   • Escort visitors and monitor visitor activity.
   • Secure keys, combinations, and other physical access devices.
   • Inventory physical access devices annually (e.g. keys, locks, card readers).
   • Change combinations and keys when combinations are compromised, keys are lost, there is a theft or security violation within the area being protected, or employees are transferred, terminated, or no longer require access.

4.15.4. Access Control for Transmission Medium (PE-4). The agency will control physical access for information system transmission and distribution lines within agency facilities.

4.15.5. Access Control for Output Devices (PE-5). The agency will control physical access to information system output devices (e.g. monitors, printers, copiers, scanners, fax machines, audio devices) to prevent unauthorized individuals from
obtaining the output. For example, place output devices within locked rooms or secured areas that can only be accessed by authorized individuals and monitored by agency personnel.

4.15.6. Monitoring Physical Access (PE-6). The agency will (i) monitor physical access to the facility where the information system resides to detect and respond to physical security incidents, (ii) monitor physical intrusion alarms and surveillance equipment, (iii) review physical access logs annually for suspicious activity such as access that is outside of normal work hours, repeated access to areas not normally accessed, or access for unusual lengths of time, and (iv) coordinate results of reviews with the agency incident response capability.

4.15.7. Visitor Access (PE-8). The agency will (i) maintain a restricted area visitor log at a designated entrance to the restricted area, (ii) require all visitors (individuals not assigned to the area) entering the restricted area to be directed to the designated entrance, (iii) maintain visitor access records to the facility where the information system resides for 5 years, and (iv) review visitor access records on an annual basis. See IRS Publication 1075 section 4.3 (restricted area access) for more information.

4.15.8. Delivery and Removal (PE-16). The agency will authorize, monitor, and control information system components entering and exiting the facility and maintain records of those items. Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

4.15.9. Alternate Work Site (PE-17). The agency will (i) employ IRS Office of Safeguards requirements at alternate work sites, (ii) assess the effectiveness of security controls at alternate work sites, and (iii) provide a means for employees to communicate with information security personnel in case of security incidents or problems. See IRS Publication 1075 section 4.7 (telework locations) for more information.

4.15.10. Location of Information System Components (PE-18). The agency will position information system components within the facility to minimize (i) potential damage from physical and environmental hazards and (ii) the opportunity for unauthorized access. Examples of physical and environmental hazards include flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, and electrical interference). See IRS Publication 1075 section 4.3 (restricted area access) and section 4.5 (physical security of computers, electronic, and removable media) for more information.
4.16. Security Planning

4.16.1. Security Planning Policy and Procedures (PL-1). The agency will develop, document, disseminate, review, and annually update a security planning policy and procedures.

4.16.2. System Security Plan (PL-2). The agency will (i) develop a Safeguard Security Report (SSR) for the information system, (ii) distribute copies of the SSR and communicate subsequent changes to the SSR to designated agency officials and the IRS Office of Safeguards, (iii) review the SSR annually and update it, as required, to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments, and (iv) protect the SSR from unauthorized disclosure and modification. An approved and accurate SSR should satisfy the requirements for the SSP identified in IRS Publication 1075 section 7.0 (reporting requirements) and:

- Is consistent with the agency’s safeguarding requirements.
- Explicitly defines information systems that receive, process, store, or transmit FTI.
- Describes the operational context of the information system in terms of missions and business processes.
- Describes the operational environment for the information system and relationships with or connections to other information systems.
- Provides an overview of the security requirements for the system.
- Identifies any relevant overlays, if applicable.
- Describes the security controls in place or planned for meeting those requirements, including a rationale for the tailoring and supplementation decisions.
- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

4.16.3. Rules of Behavior (PL-4). The agency will (i) establish and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior regarding information and information system usage, (ii) receive a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system, (iii) review and update the rules of behavior annually, (iv) require individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are updated, and (v) include in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting agency information on public websites - the IRS Office of Safeguards prohibits sharing FTI using social media/networking sites. FTI and other sensitive data will not be posted on social media, networking, or other public websites. See ETSS Technology Acceptable Use Policy 00-02 and ETSS Social Networking Policy 10-09 for more information.
4.17. Personnel Security

4.17.1. Personnel Security Policy and Procedures (PS-1). The agency will develop, document, disseminate, review, and annually update a personnel security policy and procedures.

4.17.2. Position Risk Designation (PS-2). The agency will (i) assign a risk designation to all agency positions, (ii) establish screening criteria for individuals filling those positions, and (iii) review and update position risk designations annually. In determining a position’s risk designation, the agency should consider physical access requirements to information system hardware or software, the ability to override or bypass security controls, and the scope of IT resources that may be impacted by security violations. See IRS Publication 1075 section 5.1.1 (background investigation minimum requirements) for more information.

4.17.3. Personnel Screening (PS-3). The agency will (i) screen individuals prior to authorizing access to the information system and (ii) rescreen individuals according to agency-defined criteria conditions that merit rescreening, such as a change in the individual’s job duties or position risk designation. See IRS Publication 1075 section 5.1.1 (background investigation minimum requirements) for more information.

4.17.4. Personnel Termination (PS-4). Upon termination of individual employment, the agency will (i) disable information system access, (ii) terminate/revoke any authenticators/credentials associated with the individual, (iii) perform an exit interview, (iv) retrieve and retain access to all agency information and security-related/information system–related property, and (v) notify agency personnel upon termination of the employee.

4.17.5. Personnel Transfer (PS-5). Upon reassignment or transfer to other agency positions, the agency will (i) review and confirm ongoing operational needs for current logical and physical access authorizations to information systems and facilities, (ii) initiate transfer or reassignment actions, (iii) modify access authorizations, as required, to correspond with any changes in operational needs, and (iv) notify designated agency personnel.

4.17.6. Access Agreements (PS-6). Prior to authorizing access to FTI, the agency will (i) document access agreements for agency information systems, (ii) review and update access agreements annually, and (iii) require individuals needing access to sign appropriate access agreements prior to being granted access and re-sign the access agreements annually to maintain access to agency information systems. Access agreements, such as non-disclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements, should require that individuals signing the agreement acknowledgement that they have read,
understand, and agree to abide by the constraints of the agreement, as well as indicate the penalties for non-compliance.

4.17.7. Third-Party Personnel Security (PS-7). The agency will (i) establish personnel security requirements, including security roles and responsibilities for third-party providers, (ii) require third-party providers to comply with personnel security policies and procedures established by the agency, (iii) document personnel security requirements; explicitly include personnel security requirements in acquisition-related documents, (iv) require third-party providers to notify the agency of any personnel transfers or terminations of third-party personnel who possess agency credentials or badges or who have information system privileges, and (v) monitor provider compliance. Third-party providers include contractors and other organizations providing information system development, IT services, outsourced applications, and network or security management.

4.17.8. Personnel Sanctions (PS-8). The agency will (i) employ a formal sanctions process for individuals failing to comply with established information security policies and procedures and (ii) notify designated agency personnel when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. The sanctions process should address corrective and disciplinary actions, civil and criminal penalties, and revocation of information system access privileges.

4.18. Risk Assessment

4.18.1. Risk Assessment Policy and Procedures (RA-1). The agency will develop, document, disseminate, review, and annually update a risk assessment policy and procedures.

4.18.2. Risk Assessment (RA-3). The agency will (i) perform a risk assessment to evaluate the level of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores, or transmits, (ii) document risk assessment results in the information system security plan, (iii) disseminate the system security plan to appropriate agency personnel, and (iv) review and update risk assessment results annually or whenever there is a significant change to the information system or its operational environment. Risk assessments should include security incident information, results of continuous monitoring and vulnerability scanning, and penetration tests (as appropriate). See NIST 800-30 for guidance on performing risk assessments.

4.18.3. Vulnerability Scanning (RA-5). The agency will:
- Perform monthly vulnerability scans on the information system and hosted applications and when new vulnerabilities potentially affecting the system or applications are identified and reported.
• Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for enumerating platforms, flaws, and improper configurations, formatting checklists and test procedures, and measuring vulnerability impact. Standards include specific functions, ports, protocols, and services that should not be accessible to users or devices, and improperly configured information flow mechanisms.

• Analyze vulnerability scan reports and results from security control assessments.
• Remediate legitimate vulnerabilities in accordance with an assessment of risk.
• Share information obtained from the vulnerability scanning process and security control assessments with designated agency officials to help eliminate similar vulnerabilities in other information systems.
• Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

4.19. System and Services Acquisition

4.19.1. System and Services Acquisition Policy and Procedures (SA-1). The agency will develop, document, disseminate, review, and annually update a system and services acquisition policy and procedures.

4.19.2. Allocation of Resources (SA-2). The agency will (i) determine, document, and allocate the resources required to protect the information system as part of the capital planning and investment control process, (ii) determine information security requirements for the information system in mission/business process planning, and (iii) establish a discrete line item for information security in agency programming and budgeting documentation.

4.19.3. System Development Life Cycle (SA-3). The agency will (i) manage the information system using a system development life cycle (SDLC) methodology that includes information security considerations, (ii) define, document, and assign individuals to information security roles and responsibilities, and (iii) integrate the agency risk management process into SDLC activities. See NIST 800-160 (systems security engineering) for more information.

4.19.4. Acquisition Process (SA-4). The agency will include, either explicitly or by reference, within acquisition contracts for the information system, system component, or information system service, (i) developmental and evaluation-related functional, strength, and assurance requirements, (ii) security-related documentation and documentation protection requirements, (iii) description of the information system development environment and environment in which the system is intended to operate, and (iv) acceptance criteria. Acquisition documents should include all required security capabilities and design/development processes. Acquisition packages will be reviewed and approved for compliance with all requirements.
4.19.5. Information System Documentation (SA-5). The agency will (i) obtain administrator and user documentation for information system, system component, or information system service, (ii) document attempts to obtain information system documentation when documentation is either unavailable or non-existent, (iii) secure documentation, as required, and (iv) distribute documentation to designated agency personnel.

Administrator documentation will describe (i) secure configuration, installation, and operation of the information system, component, or service, (ii) effective use and maintenance of security functions/mechanisms, and (iii) known vulnerabilities regarding configuration and use of administrative and other privileged functions.

User documentation will describe (i) user-accessible security functions and mechanisms, and how to effectively use them, (ii) methods for user interaction with the information system, component, or service, which enables individuals to use the system in a more secure manner, and (iii) user responsibilities in maintaining the security of the system, service, or component.

4.19.6. Security Engineering Principles (SA-8). The agency will apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system. The application of security engineering principles should be integrated into the SDLC targeting information systems under development, undergoing major upgrades, including legacy information systems. See NIST 800-160 (systems security engineering) for more information. Security engineering principles include:

- Developing layered protections.
- Establishing sound security policy, architecture, and controls as the foundation for design.
- Incorporating security requirements into the system development lifecycle.
- Delineating physical and logical security boundaries.
- Ensuring that system developers are trained on how to build secure software.
- Tailoring security controls to meet agency and operational needs.
- Performing threat modeling to identify use cases, threat agents, attack vectors, attack patterns, as well as compensating controls and design patterns necessary to mitigate risk.
- Reducing risk to acceptable levels.

4.19.7. External Information System Services (SA-9). The agency will:

- Prohibit the use of non-agency-owned information systems, system components, or devices that receive, process, store, or transmit FTI unless explicitly approved by the IRS Office of Safeguards. See IRS Publication 1075 section 7.4.5 (non-agency-owned information systems) for notification requirements.
- Require providers of external information system services comply with agency information security requirements, as well as security requirements of IRS Publication 1075 and other applicable federal laws, Executive Orders, directives,
policies, regulations, standards, and established service-level agreements. Service level agreements (SLA) should define expectations of performance for each required security control, describe measurable outcomes, and specify remedies and response requirements for any identified instance of non-compliance.

- Define and document government oversight, as well as user roles and responsibilities, with regard to external information system services.
- Monitor external provider security control compliance on an ongoing basis. Any identified risk that arises from the use of external information system services must be mitigated to reduce risk to an acceptable level.
- Restrict the location of information systems that receive, process, store, or transmit FTI to areas within the United States.

4.19.8. Developer Configuration Management (SA-10). The agency will require the developer of the information system, system component, or information system service to (i) perform configuration management during development, implementation, and operation of the system, component, or service, (ii) document, manage, and control the integrity of changes, (iii) only implement agency-approved changes, (iv) document approved changes and potential security impacts of the changes, and (v) track security flaws and flaw resolution, and report findings to designated agency personnel.

4.19.9. Developer Security Testing and Evaluation (SA-11). The agency will require the developer of the information system, system component, or information system service to (i) create and implement a security assessment plan, (ii) perform security testing and evaluation, (iii) produce evidence of the execution of the security assessment plan and the results of the security testing and evaluation process, (iv) implement a verifiable flaw remediation process, and (v) correct flaws identified during the security testing and evaluation process.

4.19.10. Unsupported System Components (SA-22). The agency will replace information system components (specifically software, security, and firmware patches or updates) when component support is no longer available from the developer, vendor, or manufacturer. The agency needs to proactively identify soon-to-be unsupported system components because unsupported systems will result in a critical finding by the IRS Office of Safeguards.

4.20. System and Communications Protection

4.20.1. System and Communications Protection Policy and Procedures (SC-1). The agency will develop, document, disseminate, review, and annually update a system and communications protections policy and procedures.

4.20.2. Application Partitioning (SC-2). The information system will be designed and configured to separate user functionality (including user interface services) from
information system management functionality the typically requires privileged access (e.g. access to administer databases, network components, workstations, servers, etc.). Separation can be accomplished via implementation of methods, such as different computers, partitions, central processing units, operating system instances, or network addresses.

4.20.3. Information in Shared Resources (SC-4). The information system will prevent unauthorized and unintended information transfer via shared system resources.

4.20.4. Denial of Service Protection (SC-5). The information system will protect against or limit the effects of Denial of Service (DoS) attacks to ensure legitimate users can access the information system. See NIST 800-61 (computer security incident handling guide) for more information.

4.20.5. Boundary Protection (SC-7). The information system will (i) monitor and control communications at the external boundary of the system and at key internal boundaries within the system, (ii) implement subnetworks for publicly accessible system components that are physically and logically separated from internal agency networks, (iii) connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with agency security architecture requirements, and (iv) prevent a remote device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. Managed interfaces, such as gateways, routers, and firewalls, deny network communications traffic by default and allow network communications traffic by exception (i.e. deny all, permit by exception policy).

The agency will (i) limit the number of external network connections to the information system, (ii) implement a secure managed interface for each external telecommunication service, (iii) establish a traffic flow policy for each managed interface, (iv) protect the confidentiality and integrity of the information being transmitted across each interface, (v) document each exception to the traffic flow policy with a supporting business need, duration of the need, and accept the associated risk, and (vi) review exceptions to traffic flow policy annually, and remove exceptions that are no longer supported by an explicit business need. See IRS Publication 1075 section 9.4.10 (network protections), NIST 800-41 (firewalls and firewall policy guide), NIST 800-77 (IPSec VPNs), and NIST 800-94 (intrusion detection and prevention systems) for more information.

4.20.6. Transmission Confidentiality and Integrity (SC-8). Information systems that receive, process, store, or transmit FTI will (i) protect the confidentiality and integrity of transmitted information and (ii) implement FIPS 140-2 cryptographic mechanisms to prevent unauthorized disclosure of FTI.
The agency will (i) ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized agency personnel, (ii) implement network monitoring capabilities to detect and monitor for suspicious network traffic, and (iii) apply transmission confidentiality and integrity controls to both internal and external networks and all types of information system components from which information can be transmitted (e.g. servers, mobile devices, notebook computers, printers, copiers, scanners, fax machines).

4.20.7. Network Disconnect (SC-10). The information system will terminate the network connection associated with a communications session at the end of the session or after thirty (30) minutes of inactivity. Termination of network connections are different from termination of user-initiated communications sessions, which address the termination of user-initiated logical sessions (see section AC-12 in this policy).

4.20.8. Cryptographic Key Establishment and Management (SC-12). The agency will establish and manage cryptographic keys for required cryptography employed within the information system. Cryptographic key management and establishment may be performed using manual procedures or automated mechanisms with supporting manual procedures. See NIST 800-56 (establishing cryptographic keys) and NIST 800-57 (managing cryptographic keys) for more information. When cryptographic protection is required, a FIPS 140-2 validated encryption module will be used (see http://csrc.nist.gov/groups/STM/cmvp/validation.html). The same public/private key pair will not be used to encrypt and digitally sign the same document file. Private keys will be protected using a strong password that meets the complexity requirements of ETSS Enterprise Password Security Policy 10-01. Digital certificates will be revoked when the private key is compromised, is no longer required, or upon a revocation request by agency management.

4.20.9. Cryptographic Protection (SC-13). The information system will implement cryptographic protections in accordance with applicable federal and state laws, Executive Orders, directives, regulations, and ETSS policies and standards. The agency should verify every three (3) years that encryption modules in use remain FIPS 140-2 validated (see http://csrc.nist.gov/groups/STM/cmvp/validation.html). Internet connections will use Transport Layer Security (TLS) protocol version 1.2 or higher to encrypt communications.

4.20.10. Collaborative Computing Devices (SC-15). The information system will prohibit remote activation of collaborative computing devices and provide an explicit indication of use to users physically present at the devices when collaborative computing devices are activated. Collaborative computing devices include cameras, microphones, networked white boards, or other similar devices that are built in or attached to computers and allow for transmission of audio or visual data.
4.20.11. **Public Key Infrastructure (PKI) Certificates (SC-17).** The agency will issue PKI certificates or obtain PKI certificates from an approved service provider. State-owned websites will use digital certificates issued by the current ETSS approved certificate authority. PKI is a system of processes and technologies that, in conjunction with digital certificates (authenticate the identity of users, devices, or services), enables data/email encryption, webpage security, and email/wireless/VPN connection authentication.

4.20.12. **Mobile Code (SC-18).** The agency will (i) define acceptable and unacceptable mobile code and mobile code technologies, (ii) establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies installed on servers or downloaded and executed on individual workstations and devices, and (iii) authorize, monitor, and control the use of mobile code within the information system. Mobile code is software that is capable of movement while embedded within email, documents, or websites (e.g. Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, VBScript).

4.20.13. **Voice over Internet Protocol (VoIP) (SC-19).** The agency will (i) establish usage restrictions and implementation guidance for VoIP technologies and (ii) authorize, monitor, and control the use of VoIP within the information system. At a minimum, • VoIP traffic will be encrypted using a FIPS 140-2 approved encryption algorithm when FTI is transmitted across the state or a public (i.e. internet) network. • VoIP network hardware (e.g. servers, routers, switches, firewalls) will be physically secured in accordance with MPS standards in section 4.4.5 of this policy.
• Firewalls will filter VoIP traffic.
• Information systems that transmit FTI to external customers via a VoIP network will be patched/hardened and periodically tested for vulnerabilities in accordance with the requirements of this policy.
• VoIP information systems will test security control implementation and operation prior to implementation and annually thereafter.
• VoIP phones will be logically secured.
• The agency will track and audit all FTI-applicable access and conversations.

4.20.14. **Session Authenticity (SC-23).** The information system will protect the authenticity of communications sessions. This control addresses communications protection at the session level versus the packet level (e.g. sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. See NIST 800-52 (use of TLS), NIST 800-77 (IPSec VPNs), NIST 800-95 (on securing web services), and NIST 800-113 (SSL VPNs) for more information.

4.20.15. **Protection of Information at Rest (SC-28).** The information system will protect the confidentiality and integrity of FTI at rest when located on storage devices that
are specific components of information systems and secondary storage devices such as disks and tape drives. FTI within non-volatile storage on deployed user workstations will be encrypted with FIPS-validated encryption during storage (regardless of location) except when no approved encryption solution is available for the specific technology. Mobile devices will be encrypted. See IRS Publication 1075 section 9.4.8 (mobile devices) for more information. Agencies may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms, file share scanning, and integrity protection. Additionally, agencies may employ security controls, such as secure offline storage in lieu of online storage, when adequate protection of information at rest cannot otherwise be achieved or when continuously monitoring to identify malicious code at rest.

4.21. System and Information Integrity

4.21.1. System and Information Integrity Policy and Procedures (SI-1). The agency will develop, document, disseminate, review, and annually update a system and information integrity policy and procedures.

4.21.2. Flaw Remediation (SI-2). The agency will (i) identify, report, and correct information system flaws, (ii) test software and firmware updates related to flaw remediation for effectiveness and potential side effects prior to installation, (iii) install security-relevant software and firmware updates, such as patches, service packs, hot fixes, and antivirus signatures, based on severity and associated risk to the confidentiality of FTI, (iv) incorporate flaw remediation into the agency configuration management process, and (v) centrally manage the flaw remediation process. See NIST 800-40 (enterprise patch management) for more information.

4.21.3. Malicious Code Protection (SI-3). The information system will automatically update malicious code protection mechanisms. The agency will (i) employ malicious code protection mechanisms at information system entry and exit points (e.g. firewalls, email/web/proxy/remote access servers, workstations, notebook computers, mobile devices) to detect and eradicate malicious code, (ii) update malicious code protection mechanisms when new releases are available in accordance with agency configuration management policy and procedures, (iii) configure malicious code protection mechanisms to perform weekly scans of the information system, perform real-time file scans from external sources, block or quarantine malicious code, and send an alert to the system administrator in response to malicious code detection, (iv) address the receipt of false positives during malicious code detection and eradication, and (v) centrally manage malicious code protection mechanisms. Malicious code includes viruses, worms, Trojan horses, and spyware. The agency should adopt a defense-in-depth strategy that integrates firewalls, screening, routers, intrusion detection systems, antivirus software, encryption, strong authentication, and cryptographic key management to ensure information security solutions and secure connections to external interfaces are
consistently enforced. See NIST 800-83 (malware incident prevention) for more information.

4.21.4. Information System Monitoring (SI-4). The agency will

- Monitor the information system to detect attacks, indicators of potential attacks, and unauthorized local, network, and remote connections.
- Identify unauthorized use of the information system.
- Deploy monitoring devices strategically within the information system (to collect agency-determined essential information) and at ad hoc locations within the system (to track specific types of transactions of interest to the agency).
- Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
- Increase information system monitoring activity when there is an indication of increased risk to agency operations and assets, individuals, other agencies, or the nation, based on law enforcement information, intelligence information, or other credible sources of information.
- Provide information system monitoring information to designated agency officials as needed.
- Analyze outbound communications traffic at the external boundary of the information system and selected interior points within the network (e.g. subnetworks, subsystems) to discover anomalies within agency information systems, including large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.
- Employ automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications.
- Implement host-based monitoring mechanisms on information systems that receive, process, store, or transmit FTI.

The information system will (i) monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions, (ii) alert designated personnel when indications of compromise or potential compromise occur, and (iii) notify designated personnel officials of detected suspicious events and take necessary actions to address suspicious events. Alerts may be generated from a variety of sources, including audit records, inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, and boundary protection devices (e.g. firewalls, gateways, routers). Alerts may be transmitted telephonically, via email messages, or text messages to designated personnel such as system administrators, business owners, system owners, or information system security officers. Information system monitoring includes both internal and external monitoring activities and may be achieved via a variety of tools and techniques, such as intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.
4.21.5. Security Alerts, Advisories, and Directives (SI-5). The agency will (i) receive information system security alerts, advisories, and directives from designated external agencies on an ongoing basis, (ii) generate internal security alerts, advisories, and directives as deemed necessary, (iii) disseminate security alerts, advisories, and directives to designated agency officials, and (iv) implement security directives in accordance with established time frames or notify the issuing agency of the degree of noncompliance.

4.21.6. Spam Protection (SI-8). The agency will (i) employ spam protection mechanisms at information system entry and exit points, such as firewalls, email/web/proxy servers, and workstations, to detect and take action on unsolicited messages and (ii) update spam protection mechanisms when new releases are available in accordance with ETSS Configuration Management Policy 10-14. Spam protection mechanisms should be centrally managed.

4.21.7. Information Input Validation (SI-10). The information system will check the validity of information inputs. For example, validating the format, syntax, parameters, and characters to ensure that strings contain no inserted executable or active content that can be mistakenly interpreted by the information system as commands, form validating inputs passed to interpreters must be prescreened to prevent the content from being unintentionally interpreted as commands.

4.21.8. Error Handling (SI-11). The information system will (i) generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries and (ii) reveal error messages only to designated personnel.

4.21.9. Information Handling and Retention (SI-12). The agency will handle and retain information within the information system and information output from the system in accordance with applicable federal and state laws, Executive Orders, directives, and ETSS policies, standards, and operational requirements.

4.21.10. Memory Protection (SI-16). The information system will implement safeguards to protect its memory from unauthorized code execution. Safeguards, such as data execution prevention and address space layout randomization, may be enforced via hardware or software controls. Systems administrators should increase the scrutiny of non-executable regions of memory memory locations that are prohibited, which are often used to launch attacks with executable code.

4.22. Program Management

4.22.1. Senior Information Security Officer (PM-2). The ETSS Chief Information Security Officer (CISO), in coordination with agency management, including the agency Director, Agency Information Manager (AIM), and Technical Support
Manager (TSM), will develop, implement, and maintain an enterprise-wide information security program.

ETSS Chief Information Security Officer (CISO)
Brian Tardiff
brian.tardiff@doit.ri.gov

5. Approval / Review Signature:

Brian Tardiff

Digitally signed by Brian Tardiff
Date: 2020.09.14 08:54:10 -04'00'

Chief Information Security Officer
Federal Tax Information Access Certification & Acceptance

I hereby certify that I have read ETSS Policy 10-11 (Federal Tax Information Access), agree to the terms laid out, and will abide by the guidelines contained therein. I am aware that, where this policy lacks specific guidance, I will refer to IRS Publication 1075 (http://www.irs.gov/pub/irs-pdf/p1075.pdf).

Print name: __________________________________

Signature: __________________________________

Date: _______________________________________