Internal Revenue Service (IRS)

Office of Safeguards

Safeguard Security Report (SSR)

Template Version 1.2

[Agency Name]

[Agency Code]

[Reporting Year]

Template Change Control: Safeguard Security Report

Version	Release Date	Summary of Changes
1.0	January 23, 2014	Initial Release
1.1	March 20, 2014	Minor grammar and format revisions (Updated to address feedback obtained during office hours)
1.2	January 14, 2015	FOIA footers and statement

This document is the property of the Internal Revenue Service and may not be disclosed outside your agency except to assist with finding remediation, coordination of vulnerabilities between agencies or to meet oversight requirements.

Further release of this document requires the express permission of the Internal Revenue Service. Requests received through a Sunshine or Information Sharing/Open Records provision should be referred to the federal Freedom of Information Act (FOIA) statute for processing with any release governed by IRS rules and procedures. State and local agencies receiving such requests should refer the requestor to the instructions on how to file a FOIA request with the IRS. Federal agencies should follow established procedures which require consultation before citing FOIA exemptions on IRS agency records, or directly refer the FOIA request to IRS for processing.

Additional guidance may be found at : http://www.irs.gov/uac/IRS-Freedom-of-Information and questions should be referred to the Safeguards mailbox at Safeguardreports@irs.gov

Table of Contents

Report Information			
Agency Name:	[Insert legal agency name]	**Agency Number:**	[Insert agency code]
		Date Submitted:	[Insert date of SSR submission]
IRS Reviewer:	[Leave blank]	**IRS Reference Number and Date Received:**	[Leave blank]

[Agency code] Safeguard Security Report [Year]

Please adhere to the following guidelines when submitting correspondence, reports, and attachments to the Office of Safeguards:

Report Guidance

- Reports must be completed using official templates provided by the Office of Safeguards. The most current template may be downloaded from IRS.GOV, keyword "Safeguards" or requested by emailing SafeguardReports@irs.gov.
- Provide a response for all sections of this report unless instructed otherwise in individual section(s) by the IRS Office of Safeguards. If a particular section does not apply, please mark the agency response as "Not Applicable or NA" and provide an explanation.
- If the report refers to external file attachments, the reference should clearly identify the filename and section contained within the attachment being referenced.
- Attachments must be named clearly and identify the associated section in the SSR.
- Attachment filenames must follow a standardized naming convention (e.g., SSR2.1, SSR3.1).
- Do not embed the attachment into the SSR.
- For sections where attachments are not requested but require the agency to demonstrate that policies and/or procedures are documented, please provide the policy or procedure title and/or identifier, version number, date of last update, executive level-approver and a 2-3 sentence description of the policy/procedure contents. The IRS will request to evaluate the document during the next onsite review.

Submission Guidance

- SSR and all attachments should be sent electronically to the Office of Safeguards using Secure Data Transfer (SDT), if the agency participates in the SDT program. If the agency does not participate in SDT or SDT is otherwise not available, these transmissions should be sent via email to the SafeguardReports@irs.gov mailbox.
- Files must be sent encrypted via IRS approved encryption techniques using the standard Safeguards password. The password may be requested by contacting SafeguardReports@irs.gov.
- Upon receipt of your report submission, you should receive two confirmation messages. The first message will be an automated response shortly after the submission. The second confirmation will be sent by an Office of Safeguards staff member and will be routed internally to the appropriate case worker. If an automated confirmation is not sent back to you, there was an error in your submission. If this occurs, please send an e-mail back to the IRS Office of Safeguards mailbox without attachments and request assistance.
- Please note that the IRS Office of Safeguards does not accept hard copy submissions.

Safeguard Security Report Certification

The Mission of the Office of Safeguards is to promote taxpayer confidence in the integrity of the tax system by ensuring the confidentiality of IRS information provided to federal, state, and local agencies.

Recipient agencies that legally receive federal tax information (FTI) directly from either the IRS or from secondary sources (e.g., Social Security Administration [SSA], Office of Child Support Enforcement [OCSE]), pursuant to IRC 6103 or by an IRS-approved exchange agreement, must have adequate programs in place to protect the data received, and comply with the requirements set forth in IRS Publication 1075, *Tax Information Security Guidelines For Federal, State and Local Agencies*.

By signing this certification, the Agency Head certifies that the Safeguard Security Report (SSR):

- Addresses all Outstanding Actions identified by the IRS Office of Safeguards from the prior year's SSR
- Accurately and completely reflects the agency's current environment for the receipt, storage, processing and transmission of FTI
- Accurately reflects the security controls in place to protect the FTI in accordance with Publication 1075

Additionally, the Agency Head certifies that by receiving FTI directly from either the IRS or from secondary sources the agency will:

- Assist the IRS Office of Safeguards in the joint effort of protecting the confidentiality of FTI
- Report all data incidents involving FTI to the IRS Office of Safeguards and TIGTA timely and cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident
- Support the on-site Safeguard review to assess agency compliance, including manual and automated compliance and vulnerability assessment testing and coordinating with information technology (IT) divisions to secure pre-approval, if needed, of automated system scanning
- Support timely mitigation of identified risk to FTI in the agency's Corrective Action Plan (CAP)

Agency Head Name	Agency Head Title
Signature	Date

1 Outstanding Actions

During review of the content of this report, the Office of Safeguards will identify sections that require update with the following year's SSR. This may be due to planned actions by the agency, controls planned or partially in place, or requests for additional information.

The following sections require agency updates in the next SSR submission.

2 Agency Information

The questions in Section 2, Agency Information must be updated annually.

2.1 Agency Director Provide the name, title, address, email address and telephone number of the agency official, including but limited to: agency director or commissioner authorized to request FTI from the IRS, the SSA, or other authorized agency.	
2.2 Safeguards Point of Contact Provide the name, title, address, email address and telephone number of the agency official responsible for implementing the safeguard procedures, including the primary IRS contact.	
2.3 IT Security Point of Contact Provide the name, title, address, email address and telephone number of the agency official responsible for implementing the safeguard procedures, including but not limited to the agency information technology security officer or equivalent.	

3 Current Period Safeguard Activities

The questions in Section 3, Current Period Safeguard Activities, pertain to the activities conducted by the agency during the specified reporting period. Section 3 must be updated annually.

Please provide all responses directly in the body if the SSR. If documentation is requested, please provide as an attachment.

3.1.1 FTI Data Received (Current Reporting Period)

Summarize the FTI received during the reporting period (both electronic and non-electronic). At a minimum, include the: source, type of file or extract, and volume of records received. This could be extracts from IRS, data from SSA, OCSE, Bureau of Fiscal Service or other agencies, ad hoc requests received electronically or in paper.

Note: The reporting period's record keeping logs required in Publication 1075 Section 3 for electronic and non-electronic data would meet this requirement.

Publication 1075: Section 3.0

Agency SSR Response:

Please remove blue template guidance text prior to submission, and include agency SSR response in this field

<<Section 3 is for reporting only on the **current** period of safeguard activities – agency responses should include:

- Source
- Name of file/extract
- Volume

An overview of the basic data types and extracts the agency stores, transmits, or processes; as well as agency policies and procedures regarding record keeping requirements, shall be reported in Safeguarding Procedures (Sections 5-8)>>

IRS Response:

3.1.2 Disposal of FTI (Current Reporting Period)

Summarize the FTI destroyed during the reporting period (both electronic and non-electronic). Include the method of destruction, media (paper, backup tapes, hard drive, etc.), and volume of records (or media) destroyed.

Note: The reporting period's record keeping logs required in Publication 1075 Section 3 for electronic and non-electronic data would meet this requirement.

Publication 1075: Section 8.0

Agency SSR Response:

IRS Response:

3.1.3 Re-disclosure of FTI Does the agency have a current (p)(2)(B) agreement(s)? Has the agency re-disclosed FTI through a (p)(2)(B) agreement? *Publication 1075: Section 11.4*	☐ Yes ☐ No ☐ Yes ☐ No If Yes, provide the agency to which FTI was provided and the number of records provided:
3.1.4 Reports of Internal Inspections Has the agency completed all inspections identified in its plan for the reporting period? Please provide copies of a representative sampling of the Inspection Reports and a narrative of the corrective actions taken (or planned) to correct any deficiencies. **Attachments:** Internal inspection reports, or sampling of *Publication 1075: Section 6.4*	☐ Yes ☐ No
Agency SSR Response:	
IRS Response:	

4 Changes to Safeguarding Procedures

The questions in Section 4, Changes to Safeguarding Procedures, pertain to any changes made by the agency during the specified reporting period. Section 4 must be updated annually.

Please provide all responses directly in the body if the SSR. If documentation is requested, please provide as an attachment.

4.1 Current Period Changes

4.1.1 Has the agency provided requested updates in this year's SSR to all sections identified as Outstanding Actions from the previous submission?	☐ Yes ☐ No
4.1.2 Has the agency received any new forms of FTI, to include extracts, MOU initiatives, or other forms of data sharing during the reporting period?	☐ Yes ☐ No If Yes, briefly describe here and update section 5.1:

4.1.3 Has the agency discontinued receipt or use of any FTI during the reporting period?	☐ Yes ☐ No If Yes, briefly describe here and update section 5.1:
4.1.4 Has the flow of FTI changed due to the addition of a business process, business unit, or new or enhanced information system?	☐ Yes ☐ No If Yes, briefly describe here and update section 5.2:
4.1.5 Has the agency conducted a review of staff with access to FTI to ensure those whose status has changed have had their physical and/or system access removed?	☐ Yes ☐ No
4.1.6 Has the agency added or changed contractors with access to FTI? If Yes, has the agency submitted the appropriate 45 day notifications to the Office of Safeguards? *Publication 1075: Section 7.4.3*	☐ Yes ☐ No ☐ Yes ☐ No If Yes, briefly describe here and update section 5.2:
4.1.7 Has the agency made any changes or enhancements to its information technology systems, to include hardware, software, IT organizational operations (movement to state run data center), or system security?	☐ Yes ☐ No If Yes, briefly describe here and update section 9.2:
4.1.8 Has the agency made any changes or enhancements to its physical security, to include: • New or additional office locations • Off-site storage or disaster recovery sites • Data centers • Changes to two-barrier protection standard?	☐ Yes ☐ No If Yes, briefly describe here and update section 9.3.11:
4.1.9 Has the agency made any changes or enhancements to its retention and disposal policy or methods (e.g. outsourced disposal to shredding company, change in shredding equipment, off-site storage procedures and changes in retention period)?	☐ Yes ☐ No If Yes, briefly describe here and update section 8:
4.1.10 Has the agency changed its use of FTI for the purpose of tax modeling? *Publication 1075: Section 7.4.3*	☐ Yes ☐ No If Yes, briefly describe here and update section 5.2:

4.2 Planned Changes

4.2.1 Is the agency planning any action that would substantially change current procedures or safeguarding considerations? Such major changes would include, but are not limited to, new computer equipment, facilities, or systems, or organizational changes.	☐ Yes ☐ No If Yes, briefly describe here:

Safeguarding Procedures

The questions in Sections 5 through 10 pertain to the procedures established and used by the agency for ensuring the confidentiality of FTI that is received, processed, stored, or transmitted to or from the agency. These sections should be updated as needed to accurately describe the procedures in place.

The IRS Office of Safeguards may request additional information be provided in subsequent SSR submissions. Those sections will be identified in the Outstanding Actions table.

Please provide all responses directly in the body of the SSR. If documentation is requested, please provide as an attachment.

5 FTI Flow and Processing

5.1 FTI Data

Document the data types and extracts the agency receives, processes, stores, or transmits to or from the agency. This could be extracts from IRS, data from SSA, OCSE, Bureau of Fiscal Service or other agencies, ad hoc requests received electronically or in paper. Please document how the agency complies with Publication 1075 record keeping requirements.

See Publication 1075 Section 3.0

Agency SSR Response:

Please remove blue template guidance text prior to submission, and include agency SSR response in this field

<<Different from Section 3.1.1: FTI Data Received (Current Reporting Period), please document all data types and extracts received, processed, stored, or transmitted by the agency. If the list provided in Section 3.1.1 (Currently Report Period) is all-inclusive, it can be referenced in Section 5.1.

Please document how the agency complies with Publication 1075 record keeping requirements.>>

IRS Response:

5.2 FTI Flow

Provide a description of the flow of FTI through the agency from its receipt through its return to the IRS or its destruction

- All business units or offices that use FTI
- How it is used or processed
- How it is protected along the way

Describe whether FTI is commingled with agency data or separated.

- If FTI is commingled with agency data, describe how the data is labeled and tracked.
- If FTI is separated from all other agency data, describe the steps that have been taken to keep it in isolation.

Describe the paper or electronic products created from FTI (e.g. letters, agency reports, data transcribed, spreadsheets, electronic database query results).

Describe where contractors are involved in the flow of FTI including, but not limited to, data processing, disposal, analysis, modeling, maintenance, etc.

Note: Off-site storage and/or disaster recovery staff, consolidated data center staff or contractor functions must be described.
Attachments: FTI flow diagram(s) [recommended]

See Publication 1075 Section 3.0

Agency SSR Response:

IRS Response:

6 System of Records

6.1 System of Records

Describe the permanent record(s) (logs) used to document requests for, receipt of, distribution of (if applicable), and disposition (return to IRS or destruction) of the FTI (including tapes or other removable media) (e.g. FTI receipt logs, transmission logs, or destruction logs in electronic or paper format.)

Note: Agencies are expected to be able to provide an "audit trail" for information requested and received, including any copies or distribution beyond the original document or media.
Attachments: Sample agency logs [recommended]

Publication 1075: Section 3.0

Agency SSR Response:

IRS Response:

7 Other Safeguards

7.1 Describe the agency's process for conducting internal inspections of headquarters, field offices, data center, offsite storage, and contractor sites. The agency must submit its internal inspection plan, detailing the timing of all internal inspections in the current year and next two years (three-year cycle).

Attachments: Internal inspection plan, or sampling of

Publication 1075: Section 6.4

Agency SSR Response:

IRS Response:

7.2 Describe the process for detecting and monitoring deficiencies identified during audits and internal inspections and how they are tracked in a Plan of Actions and Milestones (POA&M).

Publication 1075: Section 6.5

Agency SSR Response:

IRS Response:

8 Disposal

8.1 Describe the method(s) of FTI disposal (when not returned to the IRS) and a sample of the destruction log. For example, burning and shredding are acceptable methods of FTI disposal. Identify the specifications for each destruction method used (e.g shred size). If FTI is returned to the IRS, provide a description of the procedures.

Note: The IRS will request a written report documenting the method of destruction and that the records were destroyed.

Attachments: Destruction/disposal log template

Publication 1075: Section 6.4

Agency SSR Response:

IRS Response:

9 Information Security Controls

The questions in Section 9, Information Security Controls, are required for all agencies that receive FTI. Sections 9.3-9.4 are mapped directly to their corresponding sections in Publication 1075 (e.g., section 9.3.13 in the SSR covers the controls discussed in Section 9.3.13 of Publication 1075).

Please provide all responses directly in the body of the SSR. If documentation is requested, please provide as an attachment.

For sections related to policy and procedures (the first control in each of the control families beginning with section 9.3.1), please provide the title of the appropriate document(s), reference or identification number(s), version/release number, review or update date(s), executive level-approver, and a short summary of the content of the document(s) as it relates to that control family.

9.1.1 Provide the name and physical address where the agency's IT equipment resides (e.g. data center, computer room). Please include any secondary and/or disaster recovery data centers where FTI is housed (multiple entries are acceptable when applicable).

Agency SSR Response:

IRS Response:

9.1.2 Describe the following pertaining to data center or computer room operations:

- Identify if the facility is operated by a consolidated state-wide data center, a private contractor, or entirely by the agency
- Describe other state agencies and/or departments that have access to this facility
- Describe whether FTI access is granted to other agencies or tribes

Agency SSR Response:

IRS Response:

9.2 Electronic Flow

Provide a description of the electronic flow of FTI within all IT equipment and network devices that process, receive, store, transmit and/or maintain the data. For each device described in the flow that stores, transmit, processes, or receives FTI, identify the following:

- Platform (e.g. Mainframe, Windows, Unix/Linux, Router, Switch, Firewall)
  - If mainframe, number of production LPARs with FTI, security software (e.g. RACF, ACF2)
  - If not mainframe, number of production servers or workstations that store or access FTI.
- Operating System (e.g. zOS v1.7, Windows 2008, Solaris 10, IOS)
- Application Software (Commercial Off The Shelf or custom) used to access FTI
- Software used to retrieve FTI (e.g. SDT (Tumbleweed), CyberFusion, Connect:Direct)

Agency SSR Response:

IRS Response:

9.3.1 Access Control (AC)

9.3.1.1 AC-1: Access Control Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.
Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.

B) Access control procedures to facilitate the policy and AC related security controls. Please include details regarding procedure review/update.
Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.1.2 AC-2: Account Management

Describe how the agency authorizes access to information systems that receive, process, store, or transmit FTI based on a valid access authorization, need-to-know permission, and under the authority to re-disclose FTI under the provisions of IRC 6103. Include how the agency:

A) Identifies and selects those accounts with access to FTI to support agency mission/business functions.
B) Assigns account managers for information system accounts.
C) Establishes conditions for group and role membership.
D) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
E) Requires approval for requests to create information system accounts.
F) Creates, enables, modifies, disables, and removes information system accounts in accordance with documented agency account management procedures.
G) Monitors the use of information system accounts.
H) Notifies account managers when accounts are no longer required, when users are terminated or transferred, or when individual information system usage or need-to-know permission changes.
I) Authorizes access to information systems that receive, process, store, or transmit FTI based on a valid access authorization, need-to-know permission, and under the authority to re-disclosed FTI under the provisions of IRC 6103.
J) Reviews accounts for compliance with account management requirements at a minimum of annually for user accounts and semi-annually for privileged accounts.
K) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
L) Automatically disables inactive accounts after 120 days of user inactivity. (CE3)

Agency SSR Response:

IRS Response:

9.3.1.3 AC-3: Access Enforcement

Describe how the agency:

A) Approves authorizations for logical access to information and system resources in accordance with applicable access control policies.
B) Implements a role-based access control policy over defined subjects and objects and controls access to FTI based upon a valid access authorization, intended system usage, and the authority to be disclosed FTI under the provisions of IRC 6103.

Agency SSR Response:

IRS Response:

9.3.1.4 AC-4: Information Flow Enforcement

Describe how the agency approves 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.

Agency SSR Response:

IRS Response:

9.3.1.5 AC-5: Separation of Duties

Describe how the agency ensures that only authorized employees or contractors (if allowed by statute) have access to FTI. Include how the agency:

A) Separates duties between individuals to prevent harmful activity without collusion.
B) Documents the roles and permissions used to separate duties.
C) Defines information system access authorizations used to support the separation of duties for users authorized access to FTI.

Agency SSR Response:

IRS Response:

9.3.1.6 AC-6: Least Privilege

Describe how the agency employs the principle of least privilege. Describe how the agency:

A) Employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with agency missions and business functions.
B) Explicitly authorizes access to FTI. (CE1)
C) Requires users of information system accounts, or roles, with access to FTI, to use non-privileged accounts or roles when accessing non-security functions. (CE2)
D) Restricts privileged accounts on the information system to a limited number of individuals with a need to perform administrative duties. (CE5)
E) Audits the execution of privileged functions. (CE9)
F) Prevents non-privileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures. (CE10)

Agency SSR Response:

IRS Response:

9.3.1.7 AC-7: Unsuccessful Login Attempts

Document how the agency limits invalid logon attempts in those information systems processing, storing, and/or transmitting FTI:

A) Document the number of consecutive invalid logon attempts allowed by a user and during what duration/time period before the user is locked out.
   Per Publication 1075, the agency must enforce a limit of three consecutive invalid logon attempts by a user during a 120-minute period.

B) Document the action taken the maximum number of attempts is reached.
   Per Publication 1075, the agency must automatically lock the account until released by an administrator.

Agency SSR Response:

IRS Response:

9.3.1.8 AC-8: System Use Notification

Before granting access to the system, describe how the agency displays an IRS-approved warning banner to users of information systems containing FTI.

A) Document how the warning banner provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, regulations, standards, and guidance. Please provide the text of the warning banner, which must include:
   - The system contains U.S. Government information,
   - Users actions are monitored and audited,
   - Unauthorized use of the system is prohibited, and
   - Unauthorized use of the system is subject to criminal and civil sanctions.

   Please note the warning banner must be applied at the application, database, operating system, and network device levels for all system components that receive, process, store, or transmit FTI. Please document if all applicable components contain the approved warning banner, and if applicable, specify those that do not contain the required banner in your response.

B) Document how the user acknowledges the warning banner prior to gaining system access. The warning banner must be retained on the screen until users acknowledge the usage conditions and take explicit actions to further access the information system.

C) Document if the information system is publicly accessible and provide warning banner language. For publicly accessible information systems, the agency must:
   - Display an IRS-approved warning banner granting further access,
   - Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities, and
   - Include a description of the authorizes uses of the system.

For sample warning banners approved by the Office of Safeguards, see Exhibit 8 of Publication 1075.

Attachments: Screenshots of applicable warning banner(s), specify components and whether or not component is publicly accessible [recommended]

Agency SSR Response:

IRS Response:

9.3.1.9 AC-11: Session Lock

Describe how the agency enforces AC policy by locking workstations and applications after a pre-defined period of user inactivity.

A) Document the duration of user inactivity the information system is configured to initiate a session lock.
Per Publication 1075, the agency must prevent further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user.

B) Document the action taken to reestablish access.
Per Publication 1075, the agency must retain the session lock until the user reestablishes access using established identification and authentication procedures.

Agency SSR Response:

IRS Response:

9.3.1.10 AC-12: Session Termination

Document if, and how the information system(s) automatically terminates a user session after a pre-defined period of inactivity.

Per Publication 1075, the agency must automatically terminate a user session after 15 minutes of inactivity.

This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect).

Agency SSR Response:

IRS Response:

9.3.1.11 AC-14: Permitted Actions without Identification or Authentication

Document if the agency permits user actions on information systems receiving, processing, storing, or transmitting FTI without identification and authentication. Examples of access without identification and authentication would be instances in which the agency maintains a publicly accessible web site for which no authentication is required. If use actions are permitted, please address the following:

A) Document how the agency identifies specific user actions that can be performed on the information system without identification or authentication consistent with agency missions/business functions. Please note, FTI may not be disclosed to individuals on the information system without identification and authentication.

B) Document and provide supporting rationale for the user actions not requiring identification or authentication.

Note: If the agency does not permit actions without identification and authentication, please document in the agency response.

Agency SSR Response:

IRS Response:

9.3.1.12 AC-17: Remote Access

Remote access is defined as any access to an agency information system by a user communicating through an external network, for example: the Internet. Any remote access where FTI is accessed over the remote connection must be performed using multi-factor authentication. Please note, FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore (outside the United States). Include how the agency:

A) Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.
B) Authorizes remote access to the information system prior to allowing such connections.
C) Authorizes and documents the execution of privileged commands and access to security-relevant information via remote access for compelling operational needs only. (CE4)
D) Monitors and controls remote access methods to information systems containing FTI. (CE1)
E) Implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions where FTI is transmitted over the remote connection. (CE2)
F) Routes all remote accesses through a limited number of managed network access control points. (CE3)

Note: If the agency does not permit remote access, please document in the agency response.

Agency SSR Response:

IRS Response:

9.3.1.13 AC-18: Wireless Access

If information system(s) storing, processing, and/or transmitting FTI can be accessed on a wireless network, document how the agency:

A) Establishes wireless access policies that define usage restrictions, configuration/connection requirements, implementation guidance for wireless access.
B) Authorizes wireless access to the information system prior to allowing such connections.
C) Employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system. (SI-4, CE14)
D) Protects wireless access to the information system using authentication and encryption. (CE1)

Additional requirements for protecting FTI on wireless networks are provided in Section 9.4.18, Wireless Networks of Publication 1075.

Note: If the agency does not permit wireless access, please document in the agency response.

Agency SSR Response:

IRS Response:

9.3.1.14 AC-19: Access Control for Mobile Devices

If FTI can be accessed and/or retrieved from a mobile or portable device, describe how the agency:

A) Establishes mobile device policies that define usage restrictions, configuration/connection requirements, implementation guidance for agency-controlled mobile devices.
B) Authorizes the connection of mobile devices to agency information systems.
C) Employs encryption to protect the confidentiality and integrity of information on mobile devices (e.g., smartphones and laptop computers). (CE5)
D) Purges/wipes information from mobile devices based on 10 consecutive, unsuccessful device logon attempts (e.g., personal digital assistants, smartphones and tablets). Laptop computers are excluded from this requirement. (AC-7, CE2)

Additional requirements on protecting FTI accessed by mobile devices are provided in Section 9.4.8, Mobile Devices of Publication 1075.

Agency SSR Response:

IRS Response:

9.3.1.15 AC-20: Use of External Information Systems

External information systems include any technology used to receive, process, transmit, or store FTI that is not owned and managed by the agency. Describe how the agency prohibits the following, unless approved by the Office of Safeguards:

A) Access to FTI from external information systems.
B) Use of agency-controlled portable storage devices (e.g., flash drives, external hard drives) containing FTI on external information systems. (CE2)
C) Use of non-agency-owned information systems, system components, or devices to process, store, or transmit FTI.
   - Non-agency owned information system usage requires the agency to notify the Office of Safeguards 45 days prior to implementation (see Section 7.4, 45-Day Notification Reporting Requirements of Publication 1075). (CE3)

Document any exceptions and/or approvals granted by the Office of Safeguards.

Agency SSR Response:

IRS Response:

9.3.1.16 AC-21: Information Sharing

Validate and describe how the agency restricts the sharing/re-disclosure of FTI to only those authorized in IRC 6103 and as approved by the Office of Safeguards.

Agency SSR Response:

IRS Response:

9.3.1.17 AC-22: Publicly Accessible Content

Describe how the agency safeguards FTI in publicly accessible information systems. Include how the agency:

A) Designates individuals authorized to post information onto a publicly accessible information system.
B) Trains authorized individuals to ensure that publicly accessible information does not contain FTI.
C) Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that FTI is not included.
D) Reviews content on publicly accessible information system(s) for FTI; and immediately removes it if and when it is discovered.

Per Publication 1075, the agency must review the content on the publicly accessible information system for FTI, at a minimum, quarterly and remove such information, if discovered.

Agency SSR Response:

IRS Response:

9.3.2 Awareness and Training (AT)

9.3.2.1 AT-1: Security Awareness and Training Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.

Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.

B) Security awareness and training procedures to facilitate the policy and AT related security controls. Please include details regarding procedure review/update.

Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.2.2 AT-2: Security Awareness Training

Describe how the agency ensures all information system users and managers are knowledgeable of security awareness material before authorizing access to the system.

A) Document how information system users (managers, senior executives, and contractors) with access to FTI receive basic security awareness training as part of initial training for new users, when required by information system changes, and at least annually thereafter. Please describe the content of security awareness training.

B) Document how the agency includes security awareness training on recognizing and reporting potential indicators of insider threat. (CE2)

Agency SSR Response:

IRS Response:

9.3.2.3 AT-3: Role Based Security Training

Describe how the agency implements role-based security training.

A) Document how the agency provides role-based training to personnel with security roles and responsibilities before authorizing access to the information system or performing assigned duties that require access to FTI, when required by information system changes, and at least annually thereafter. Please describe the content of role-based security training.

Agency SSR Response:

IRS Response:

9.3.2.4 AT-4: Security Training Records

Document how the agency monitors and maintains security training records.

A) Describe how the agency documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

B) Define the duration in which individual training records are retained.

Per Publication 1075, the agency must retain individual training records for a period of five years.

Agency SSR Response:

IRS Response:

9.3.3 Audit and Accountability (AU)

9.3.3.1 AU-1: Audit and Accountability Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.
   Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.

B) Audit and accountability procedures to facilitate the policy and AU related security controls. Please include details regarding procedure review/update.
   Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.3.3 AU-2: Audit Events

Describe how the agency's information system(s) generate audit records for all security-relevant events. Security-relevant events must 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. Access to FTI must be audited at the information system, operating system, software, and database levels.

A) Document which event types are audited by the information system and all supporting components storing, processing, or transmitting FTI.

Per Publication 1075, at a minimum, the information system shall audit the following event types: Log onto the system, log off the system, change of password, all system administrator commands (while logged on as system administrator), switching accounts or running privileged actions from another account (e.g., Linux/Unix SU or Windows RUNAS), the creation or modification of super-user groups, subset of security administrator commands (while logged on in the security administrator role), subset of system administrator commands (while logged on in the user role), clearing of the audit log file, startup and shutdown of audit functions, use of identification and authentication mechanisms (e.g., user ID and password), change of file or user permissions or privileges (e.g., use of suid/guid,chown, su), remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system, changes made to an application or database by a batch file, application-critical record changes, changes to database or application records (where the application has been bypassed to produce the change [via a file or other database utility]), all system and data interactions concerning FTI, and any additional platform-specific events, as defined in SCSEMs located on the Office of Safeguards website.

B) Document how the agency coordinates the security audit functions with other agency entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

C) Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

D) Document the duration in which the list of audited events is reviewed and updated. (CE3)

Per Publication 1075, the agency must review and update the audited events at a minimum, annually.

Agency SSR Response:

IRS Response:

9.3.3.4 AU-3: Content of Audit Records

Describe how the agency's identified security-relevant events enable the detection of unauthorized access to FTI data.

A) Document the audit record content that is captured by the information system and all supporting components storing, processing, or transmitting FTI.

Per Publication 1075, at a minimum, the agency must generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

B) Document details of the agency's audit records (for all applicable components) that contain information to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected in the audit records for audit events identified by type, location, or subject. (CE1)

Agency SSR Response:

IRS Response:

9.3.3.5 AU-4: Audit Storage Capacity

Describe how the agency configures information systems containing FTI to allocate sufficient audit record storage capacity. Per Publication 1075, the agency must allocate audit record storage capacity to retain audit records for the required audit retention period of seven years.

Agency SSR Response:

IRS Response:

9.3.3.6 AU-5: Response to Audit Processing Failures

Describe how the agency responds to audit processing failures.

A) Document how the agency alerts designated agency officials in the event of an audit processing failure.

B) Document how the agency monitors system operational status using operating system or system audit logs, and verifies functions and performance of the information system.

- Logs shall be able to identify where system process failures have taken place and provide information relative to corrective actions to be taken by the system administrator.

C) Document if and how automated warnings are provided when allocated audit record storage volume reaches (or exceeds) a maximum audit storage records capacity. (CE1)

Agency SSR Response:

IRS Response:

9.3.3.7 AU-6: Audit Review, Analysis, and Reporting

Describe how the agency reviews audit records for indications of unusual activities, suspicious activities or suspected violations.

A) Define the frequency in which audit records are reviewed and analyzed.
   Per Publication 1075, the agency must review and analyze information system audit records at least weekly or more frequently at the discretion of the information system owner for indications of unusual activity related to potential unauthorized FTI access.

B) Document how findings are reported.
   Per Publication 1075, findings shall be reported in accordance with the agency incident response policy; If the finding involves a potential unauthorized disclosure of FTI, the appropriate special agent-in-charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards must be contacted, as described in Section 10.0: *Reporting Improper Inspections or Disclosures*, of Publication 1075.

Refer to Table 8: Proactive Auditing Methods to Detect Unauthorized Access to FTI, of Publication 1075 for recommended proactive audit methods.

Agency SSR Response:

IRS Response:

9.3.3.8 AU-7: Audit Reduction and Report Generation

Describe how the agency's information system(s) provide an audit reduction and report generation capability to enable review of audit records.

A) Document how the agency supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents.

B) Document how the agency ensures the original content or time ordering of audit records is not altered.

Agency SSR Response:

IRS Response:

9.3.3.9 AU-8: Time Stamps

Describe how the agency's information system(s) provides date and time stamps in audit record generation.

A) Document if, and what internal system clocks are used to generate time stamps for audit records.

B) Document how the agency records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

C) Document if the agency compares and synchronizes the internal information system clocks to approved authoritative time sources (e.g., NIST, Naval Observatory). (CE1)

Agency SSR Response:

IRS Response:

9.3.3.10 AU-9: Protection of Audit Information

Describe how the agency's information system(s) protects audit information.

A) Document how the agency's information systems protect audit information and audit tools from unauthorized access, modification, and deletion.

B) Document if, and how the agency authorizes access to manage audit functionality only to designated security administrator(s) or staff other than the system and network administrator. System and network administrators must not have the ability to modify or delete audit log entries. (CE4)

Agency SSR Response:

IRS Response:

9.3.3.11 AU-11: Audit Record Retention

Describe how the agency ensures audit information is archived to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements.

Per Publication 1075, the agency must retain audit records for 7 years.

Agency SSR Response:

IRS Response:

9.3.3.12 AU-12: Audit Generation

Describe the audit generation capabilities for the information system and all supporting components storing, processing, or transmitting FTI. Include how the information system:

A) Provides audit generation capabilities for all auditable events defined in Section 9.3.3.2 (AU-2: Auditable Events).

B) Allows designated agency officials to select which auditable events are to be audited by specific components of the information system.

C) Generates audit records with the content defined in Section 9.3.3.4 (AU-3: Content of Audit Records).

Agency SSR Response:

IRS Response:

9.3.3.13 AU-16: Cross-Agency Auditing

Describe how the agency employs mechanisms for coordinating the access and protection of audit information among external entities when audit information is transmitted across agency boundaries.

- This requirement applies to outsourced data centers or cloud providers. The provider must be held accountable to protect and share audit information with the agency through the contract. Refer to Section 9.4.1, Cloud Computing Environments, and Section 5.4, Controls over Processing, of Publication 1075 for additional requirements.

Agency SSR Response:

IRS Response:

9.3.4 Security Assessment and Authorization (CA)

9.3.4.1 CA-1: Security Assessment and Authorization Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) A security assessment and authorization (SA&A) policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.

Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.

B) Security assessment and authorization procedures to facilitate the policy and CA related security controls. Please include details regarding procedure review/update.

Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Note: For federal agencies that receive FTI, a NIST compliant SA&A is required in accordance with FISMA. For state or local agencies that receive FTI, a third-party accreditation is not required. Instead these agencies may internally attest.

Agency SSR Response:

IRS Response:

9.3.4.2 CA-2: Security Assessments

Describe how the agency conducts an assessment of the security controls in the information system to ensure the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

A) Document how the agency develops and a security assessment plan that contains the scope of the assessment (selected security controls, applicable environments, and assessment roles and responsibilities), and assessment procedures.

B) Document how the agency assesses security controls applicable to the information system and its environment to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

Per Publication 1075, the agency must assess security controls at a minimum of an annual basis.

C) Document if the agency produces a security assessment report that documents the results of the assessment.

D) Document how the agency provides results to the agency's Authorizing Official.

Agency SSR Response:

IRS Response:

9.3.4.3 CA-3: System Interconnections

Describe how the agency protects and monitors information system interconnections.

A) Document how the agency authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements (ISA).

B) Document the content of ISA language, including but not limited to: the interface characteristics, security requirements, and the nature of the information transmitted.

C) Document how often the agency reviews and updates the system interconnections.

Per Publication 1075, the agency must review and update the system interconnection on an annual basis.

D) Describe how the agency employs a deny-all and allow-by-exception policy for allowing systems that receive, process, store, or transmit FTI to connect to external information systems. (CE5)

Agency SSR Response:

IRS Response:

9.3.4.4 CA-5: Plan of Action and Milestones

Describe how the agency develops and updates a Plan of Action & Milestones that identifies any deficiencies (identified in the agency Corrective Agency Plan [CAP], through security control assessments, and continuous monitoring activities) related to FTI processing.

A) Document if the agency develops a POA&M for the information system to document the agency's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of security controls (from CA-2: Security Assessment) and to reduce or eliminate known vulnerabilities in the system.

B) Define the frequency in which the POA&M is reviewed and updated by the agency.

Per Publication 1075, the agency must update the existing POA&M, at a minimum, on a quarterly basis.

The POA&M must comprise an all-inclusive tool or document for the agency to track vulnerabilities identified by the self-assessments, continuous monitoring activities, internal inspections, external audits and any other vulnerabilities identified for information systems that receive, process, store, or transmit FTI. Refer to Section 6.5, Plan of Action and Milestones, of Publication 1075 for additional information.

Agency SSR Response:

IRS Response:

9.3.4.5 CA-6: Security Authorization

Describe how owners of FTI authorize the security controls used to protect FTI before initiating operations. Include how the agency:

A) Assigns a senior-level executive or manager as the authorizing official for the information system.

B) Ensures that the authorizing official authorizes (through signature approval) the information system for processing before commencing operations.

C) Updates the security authorization whenever there is a significant change to the system, or every three years, whichever occurs first.

Agency SSR Response:

IRS Response:

9.3.4.6 CA-7: Continuous Monitoring

Describe how the agency has developed an information security continuous monitoring (ISCM) strategy and program. The strategy shall include the following:

A) Establishment of agency-defined metrics to be monitored on a regular basis.
   Per Publication 1075, agency defined metrics shall be monitored at least annually.
B) Ongoing security control assessments in accordance with the agency continuous monitoring strategy.
C) Ongoing security status monitoring of agency-defined metrics in accordance with the agency continuous monitoring strategy.

In accordance with the agency ISCM strategy, document how the agency conducts ongoing security control assessments within the information system(s) hosting FTI and facilitates ongoing security status monitoring of agency-defined metrics.

Agency SSR Response:

IRS Response:

9.3.5 Configuration Management (CM)

9.3.5.1 CM-1: Configuration Management Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.
   Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.
B) Configuration management procedures to facilitate the policy and CM related security controls. Please include details regarding procedure review/update.
   Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.5.2 CM-2: Baseline Configuration

Describe how the agency develops and maintains a baseline configuration for information system components.

A) Document how the agency develops, documents, and maintains under configuration controls, a current baseline configuration of the information system.

B) Document the agency's frequency of review and update of the baseline configuration of the information system. (CE1)

Per Publication 1075, the agency must review or update the baseline, at a minimum, annually; when required due to system upgrades, patches, or other significant changes; and as an integral part of information system component installations and upgrades.

The Office of Safeguards recommends using SCSEMs provided on the Office of Safeguards website for developing an information system baseline configuration.

Agency SSR Response:

IRS Response:

9.3.5.3 CM-3: Configuration Change Control

Describe how the agency authorizes, documents, and controls changes to the information system. Include how the agency addresses:

A) Determines the types of changes to the information system that are configuration controlled.

B) Reviews proposed configuration-controlled changes to the information system; and approves or disapproves such changes with explicit consideration for security impact analyses.

C) Documents configuration change decisions associated with the information system.

D) Implements approved configuration-controlled changes to the information system.

E) Retains records of configuration-controlled changes to the information system for the life of the system.

F) Audits and reviews activities associated with configuration-controlled changes to the information system.

G) Coordinates and provides oversight for configuration change control activities through a Configuration Control Board that convenes when configuration changes occur.

H) Tests, validates, and documents changes to the information system before implementing the changes on the operational system. (CE2)

Agency SSR Response:

IRS Response:

9.3.5.4 CM-4: Security Impact Analysis

Describe how the agency analyzes changes to the information system to determine potential security impacts prior to change implementation.

Agency SSR Response:

IRS Response:

9.3.5.5 CM-5: Access Restrictions for Change

Describe how the agency defines, documents, approved, and enforces physical and logical access restrictions associated with changes to the information system.

Agency SSR Response:

IRS Response:

9.3.5.6 CM-6: Configuration Settings

Describe how the agency establishes configuration settings and monitors agency compliance. Include how the agency:

A) Establishes and documents configuration settings for IT products that receive, process, store, or transmit FTI using Office of Safeguards–approved compliance requirements (e.g., SCSEMs, assessment tools) that reflect the most restrictive mode consistent with operational requirements.
B) Implements the configuration settings.
C) Identifies, documents, and approves any deviations from established configuration settings for information systems that receive, process, store, or transmit FTI.
D) Monitors and controls changes to the configuration settings in accordance with agency policies and procedures.

Note: The authoritative source for platform checklists used by the Office of Safeguards is the NIST Checklist Program Repository (http://checklists.nist.gov).

Agency SSR Response:

IRS Response:

9.3.5.7 CM-7: Least Functionality

Describe how the agency implements least functionality in its information systems. Include how the agency:

A) Configures the information system to provide only essential capabilities.
B) Prohibits or restricts the use of the functions, ports, protocols, or services as defined in Office of Safeguards–approved compliance requirements (e.g., SCSEMs, assessment tools).
C) Reviews the information system as part of vulnerability assessments to identify unnecessary or non-secure functions, ports, protocols, and services (see Section 9.3.14.3, Vulnerability Scanning (RA-5), of Publication 1075).
D) Disables defined functions, ports, protocols, and services within the information system deemed to be unnecessary or non-secure.

Agency SSR Response:

IRS Response:

9.3.5.8 CM-8: Information System Component Inventory

Describe how the agency develops and maintains an inventory of information system components.

A) Document how the agency develops and documents an inventory of information system components that: accurately reflects the current information system; includes all components that store, process, or transmit FTI; is at the level of granularity deemed necessary for tracking and reporting; and includes information deemed necessary to achieve effective information system component accountability.
B) Document how the agency reviews and updates the information system component inventory through periodic manual inventory checks or a network monitoring tool that automatically maintains the inventory.
C) Document how the agency updates the inventory of information system components as an integral part of component installations, removals, and information system updates. (CE1)

Additional requirements for maintaining a system component inventory are provided in Section 9.4.12, System Component Inventory, of Publication 1075.

Agency SSR Response:

IRS Response:

9.3.5.9 CM-9: Configuration Management Plan

Describe how the agency develops, documents, and implements a configuration management plan (CMP) for the information system. The CMP shall:

- Address roles, responsibilities, and configuration management processes and procedures,
- Establish a process for identifying configuration items throughout the system development life cycle (SDLC) and for managing the configuration of the configuration items,
- Define the configuration items for the information system and places the configuration items under configuration management, and
- Be protected from unauthorized disclosure and modification.

Agency SSR Response:

IRS Response:

9.3.5.10 CM-10: Software Usage Restrictions

Describe how the agency establishes and monitors software usage restrictions. Include how the agency:

A) Uses software and associated documentation in accordance with contract agreements and copyright laws.
B) Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution.
C) Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
D) Establishes restrictions on the use of open source software. Open source software must be: legally licensed; approved by the agency IT department; and adhere to a secure configuration baseline checklist from the U.S. Government or industry. (CE1)

Agency SSR Response:

IRS Response:

9.3.5.11 CM-11: User-Installed Software

Describe how the agency addresses and monitors the installation of software by users.

A) Document the policies the agency has established to govern the installation of software by users.
B) Describe how the agency enforces software installation policies through automated methods.
C) Describe how the agency monitors policy compliance on a continual basis.

Agency SSR Response:

IRS Response:

9.3.6 Contingency Planning (CP)

9.3.6.1 CP-1: Contingency Planning Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.
Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.

B) Contingency planning procedures to facilitate the policy and CP related security controls. Please include details regarding procedure review/update.
Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Note: All FTI that is transmitted to agencies is backed up and protected within IRS facilities. As such, the focus of contingency planning controls is on the protection of FTI stored in agency owned or managed backup media or used at alternative facilities and not focused on the availability of data. If FTI is included in contingency planning – policy and procedures must be developed, documented, disseminated, and updated as necessary to facilitate implementing contingency planning security controls.

Agency SSR Response:

IRS Response:

9.3.6.2 CP-2: Contingency Plan

If FTI is included in contingency planning, describe how the agency develops and maintains a contingency plan for the information system. The contingency plan shall:

- Identify essential missions and business functions and associated contingency requirements;
- Provide recovery objectives, restoration priorities, and metrics;
- Address contingency roles, responsibilities, and assigned individuals with contact information;
- Address maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
- Address eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented;
- Be reviewed and approved by designated agency officials;
- Be distributed to key contingency personnel;
- Be coordinated with incident handling activities;
- Be reviewed at least annually;
- Be updated to address changes to the agency, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing. Changes shall be communicated to key contingency personnel; and
- Be protected from unauthorized disclosure and modification.

Agency SSR Response:

IRS Response:

9.3.6.3 CP-3: Contingency Training

Describe how personnel are trained in their contingency roles and responsibilities with respect to the information system. Per Publication 1075, testing shall occur prior to assuming a contingency role or responsibility, when required by information system changes, and annually thereafter.

Agency SSR Response:

IRS Response:

9.3.6.4 CP-4: Contingency Plan Testing

Describe how the agency tests contingency plans to determine the effectiveness of the plan and the agency's readiness to execute the plan.

A) Document how the agency tests the contingency plan for the information system, and define the frequency. Per Publication 1075, the agency shall test the contingency plan, at a minimum, annually.
B) Document how the agency reviews contingency plan test results.
C) Document how the agency initiates corrective actions, if/when needed.

Agency SSR Response:

IRS Response:

9.3.6.5 CP-6: Alternate Storage Site

Describe how the agency identifies alternate storage sites.

A) Document how the agency establishes necessary agreements to permit the secure storage and retrieval of information system and FTI backups.
B) Document how the agency ensures the alternate storage site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103.

Agency SSR Response:

IRS Response:

9.3.6.6 CP-7: Alternate Processing Site

Describe how the agency identifies alternate processing sites.

A) Describe how the agency establishes an alternate processing site, including necessary agreements to permit the transfer and resumption of information system operations, in accordance with the agency's contingency plan when the primary processing capabilities are unavailable.

B) Describe how the agency ensures 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 the agency-defined time period for transfer/resumption.

C) Document how the agency ensures the alternate processing site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103.

Agency SSR Response:

IRS Response:

9.3.6.7 CP-9: Information System Backup

Describe how the agency conducts and protect information system backups containing FTI.

A) Document how the agency conducts backups of user-level information, system-level information, and security-related documentation consistent with the defined frequency in the agency's contingency plan.

B) Document how the agency protects the confidentiality of backup information at storage locations pursuant to IRC 6103 requirements.

Agency SSR Response:

IRS Response:

9.3.6.8 CP-10: Information System Recovery and Reconstitution

Describe how the agency provides and enables the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Agency SSR Response:

IRS Response:

9.3.7 Identification and Authentication (IA)

9.3.7.1 IA-1: Identification and Authentication Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.

Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.

B) Identification and authentication procedures to facilitate the policy and IA related security controls. Please include details regarding procedure review/update.

Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.7.2 IA-2: Identification and Authentication (Organizational Users)

Describe how the agency identifies and authenticates organizational users accessing FTI.

A) Document how the agency uniquely identifies and authenticates organizational/agency users (or processes acting on behalf of agency users).

B) Document if, and how the agency implements multi-factor authentication for all remote network access to privileged and non-privileged accounts for information systems that receive, process, store, or transmit FTI. (CE1, CE2)

C) Document if, and how the agency implements 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. NIST SP 800-63 allows the use of software tokens. (CE11)

Agency SSR Response:

IRS Response:

9.3.7.3 IA-3: Device Identification and Authentication

Describe how the agency uniquely identifies and authenticates devices before establishing a connection.

Agency SSR Response:

IRS Response:

9.3.7.4 IA-4: Identifier Management

Describe how the agency manages user accounts and information system identifiers.

A) Describe how the agency requests and receives authorization from designated agency officials to assign an individual, group, role, or device identifier.
B) Describe how the agency selects an identifier that identifies an individual, group, role, or device.
C) Describe how the agency assigns the identifier to the intended individual, group, role, or device.
D) Describe how the agency prevents reuse of identifiers.
E) Describe if, and how the agency disables information system identifiers after a period of user inactivity.
Per Publication 1075, the agency must disable the identifier after 120 days of user inactivity.

Agency SSR Response:

IRS Response:

9.3.7.5 IA-5: Authenticator Management

Describe how the agency manages information system authenticators (or passwords). Describe how the agency implements the following authenticator requirements:

A) Verifies, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.
B) Establishes initial authenticator content for authenticators defined by the agency.
C) Ensures authenticators have sufficient strength of mechanism for their intended use.
D) Establishes and implements administrative procedure(s) for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
E) Changes default content of authenticators prior to information system installation.
F) Establishes minimum and maximum lifetime restrictions and reuse conditions for authenticators.
G) Changes/refreshes authenticators on a regular basis (include frequency in agency response).
H) Protects authenticator content from unauthorized disclosure and modification.
I) Requires individuals to take, and having devices implement, specific security safeguards to protect authenticators.
J) Changes authenticators for group/role accounts when membership to those accounts changes.
K) Describe how the information system, for password-based authentication: enforces minimum password complexity of: 8 characters; at least one numeric and at least one special character; mixture of at least one uppercase and at least one lowercase letter; and stores and transmits only encrypted representations of passwords.
L) Enforces password minimum lifetime restriction of one day.
M) Enforces non-privileged account passwords to be changed at least every 90 days.
N) Enforces privileged account passwords to be changed at least every 60 days.
O) Prohibits password reuse for 24 generations.
P) Allows the use of a temporary password for system logons requiring an immediate change to a permanent password.
Q) Password-protects system initialization (boot) settings.

Agency SSR Response:

IRS Response:

9.3.7.6 IA-6: Authenticator Feedback

Describe how the agency's information system(s) obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Agency SSR Response:

IRS Response:

9.3.7.7 IA-7: Cryptographic Module Authentication

Describe how the agency ensures cryptographic modules are compliant with NIST guidance, including FIPS 140-2 compliance.

Per Publication 1075, the information system must implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. Validation provides assurance that when agency implements cryptography to protect FTI, the encryption functions have been examined in detail and will operate as intended.

All electronic transmissions of FTI must be encrypted using FIPS 140-2 validated cryptographic modules. A product does not meet the FIPS 140-2 requirements by simply implementing an approved security function. Only modules tested and validated to FIPS 140-2 meet the applicability requirements for cryptographic modules to protect sensitive information. NIST maintains a list of validated cryptographic modules on its website http://csrc.nist.gov/.

Agency SSR Response:

IRS Response:

9.3.7.8 IA-8: Identification and Authentication (Non-Organizational Users)

Describe how the agency uniquely identifies and authenticates non-agency users (or processes acting on behalf of non-agency users).

Agency SSR Response:

IRS Response:

9.3.8 Incident Response (IR)

9.3.8.1 IR-1: Incident Response Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.
   Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.

B) Incident response procedures to facilitate the policy and IR related security controls. Please include details regarding procedure review/update.
   Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.8.2 IR-2: Incident Response Training

Describe how the agency trains personnel with access to FTI, including contractors and consolidated data center employees if applicable, in their incident response roles on the information system and FTI. Document if, and how the agency provides incident response training to information system users consistent with assigned roles and responsibilities. In your response please document if incident response training occurs:

A) Prior to assuming an incident response role or responsibility;
B) When required by information system changes; and
C) Annually thereafter.

Agency SSR Response:

IRS Response:

9.3.8.3 IR-3: Incident Response Testing

Describe how the agency tests and/or exercises the incident response capability for the information system on at least an annual basis.

A) Describe how the agency performs tabletop exercises using scenarios that include a breach of FTI, and tests the agency's incident response policies and procedures.
B) Document if all employees and contractors with significant FTI incident response capabilities, including technical personnel responsible for maintaining consolidated data centers and off-site storage, are included in tabletop exercises.
C) Describe how the agency produces an after-action report for each tabletop exercise to improve existing processes, procedures, and policies.

Refer to Section 10.3, Incident Response Procedures, for specific instructions on incident response requirements where FTI is involved.

Agency SSR Response:

IRS Response:

9.3.8.4 IR-4: Incident Handling

Describe how the agency implements an incident handling capability. Document how the agency conducts the following:

A) Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
B) Coordinates incident handling activities with contingency planning activities; and
C) Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implement the resulting changes accordingly.

Agency SSR Response:

IRS Response:

9.3.8.5 IR-5: Incident Monitoring

Describe how the agency routinely tracks and documents all physical and information system security incidents potentially affecting the confidentiality of FTI.

Agency SSR Response:

IRS Response:

9.3.8.6 IR-6: Incident Reporting

Describe the agency's policy to report incidents when there is a compromise to FTI. Document how the agency conducts the following:

A) Requires personnel to report suspected security incidents to internal agency incident response resources upon discovery of the incident.
B) Contacts the appropriate special agent-in-charge, TIGTA, and the IRS Office of Safeguards immediately but no later than 24 hours after identification of a possible issue involving FTI.

Please refer to Section 10: Reporting Improper Inspections or Disclosures, for more information on incident reporting requirements required by the Office of Safeguards.

Agency SSR Response:

IRS Response:

9.3.8.7 IR-7: Incident Response Assistance

Describe how the agency provides an incident response support resource (e.g. help desk) that offers advice and assistance to users of the information system containing FTI and/or users with physical access to FTI. Describe how the support resource is an integral part of the agency's incident response capability.

Agency SSR Response:

IRS Response:

9.3.8.8 IR-8: Incident Response Plan

Describe how the agency develops and maintains an Incident Response Plan (IRP). Please include how the agency:

A) Develops and maintains an incident response plan that:
- Provides the agency with a roadmap for implementing its incident response capability;
- Describes the structure of the incident response capability;
- Provides a high-level approach for how the incident response capability fits into the overall agency;
- Meets the unique requirements of the agency, which related to mission, size, structure, and functions;
- Defines reportable incidents;
- Provides metrics for measuring the incident response capability within the agency;
- Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
- Ensures the document is reviewed and approved by designated agency officials.

B) Distributes to authorized incident response personnel and protected from unauthorized disclosure and modification.
C) Reviews the IRP, at a minimum, on an annual basis or as an after-action review.
D) Updates the IRP to address system/agency changes or problems encountered during plan implementation, execution, or testing.
E) Communicates IRP changes to authorized incident response personnel.
F) Protects the IRP from unauthorized disclosure and modification.

Agency SSR Response:

IRS Response:

9.3.8.9 IR-9: Information Spillage Response

Describe how the agency responds to information spills. Include how the agency:

A) Identifies the specific information involved in the information system contamination.
B) Alerts authorized incident response personnel of the information spill using a method of communication not associated with the spill.
C) Isolates the contaminated information system or system component.
D) Eradicates the information from the contaminated information system or component.
E) Identifies other information systems or system components that may have been subsequently contaminated.

Agency SSR Response:

IRS Response:

9.3.9 Maintenance (MA)

9.3.9.1 MA-1: System Maintenance Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.
   Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.
B) System maintenance procedures to facilitate the policy and MA related security controls. Please include details regarding procedure review/update.
   Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.9.2 MA-2: Controlled Maintenance

Describe how the agency ensures system maintenance is scheduled, performed, and documented.

A) Describe how the agency schedules, performs, documents, and reviews records of maintenance and repairs on information system components of the information system in accordance with manufacturer or vendor specifications and agency requirements.

B) Describe how the agency approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

C) Describe how the agency requires designated agency officials to explicitly approve the removal of the information system or system components from agency facilities for off-site maintenance or repairs.

D) Describe how the agency sanitizes equipment to remove all FTI from associated media prior to removal from agency facilities for off-site maintenance or repairs.

E) Describe how the agency checks and confirms the implementation of potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions and update agency maintenance records accordingly.

Agency SSR Response:

IRS Response:

9.3.9.3 MA-3: Maintenance Tools

Describe how the agency approves, controls, and monitors information system maintenance tools.

Agency SSR Response:

IRS Response:

9.3.9.4 MA-4: Non-Local Maintenance

Describe how the agency controls and monitors non-local maintenance. Include how the agency:

A) Approves, controls, and monitors non-local maintenance and diagnostic activities.

B) Allows the use of non-local maintenance and diagnostic tools only as consistent with agency policy and documented in the security plan for the information system.

C) Employs multi-factor authenticator in the establishment of non-local maintenance and diagnostic sessions.

D) Maintains records for non-local maintenance and diagnostic activities.

E) Terminates session and network connections when non-local maintenance is completed.

F) Documents policies and procedures for the establishment and use of non-local maintenance and diagnostic connections. (CE2)

Agency SSR Response:

IRS Response:

9.3.9.5 MA-5: Maintenance Personnel

Describe how the agency allows only authorized personnel to perform maintenance on the information system. Include how the agency:

A) Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel.
B) Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations.
C) Designates agency personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Agency SSR Response:

IRS Response:

9.3.10 Media Protection (MP)

9.3.10.1 MP-1: Media Protection Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.
   Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.
B) Media protection procedures to facilitate the policy and MP related security controls. Please include details regarding procedure review/update.
   Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Note: Information system media is defined to include both digital (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs) and non-digital (e.g., paper).

Agency SSR Response:

IRS Response:

9.3.10.2 MP-2: Media Access

Where information system digital and non-digital media contains FTI, describe how the agency restricts access to authorized individuals.

Agency SSR Response:

IRS Response:

9.3.10.3 MP-3: Media Marking

Describe how the agency labels information system media containing FTI to indicate the distribution limitations and handling caveats.

Per Publication 1075, the agency must label removable media (CDs, DVDs, diskettes, magnetic tapes, external hard drives and flash drives) and information system output containing FTI (reports, documents, data files, back-up tapes) indicating "Federal Tax Information". Notice 129-A and Notice 129-B IRS provided labels can be used for this purpose.

Agency SSR Response:

IRS Response:

9.3.10.4 MP-4: Media Storage

Describe how the agency protects the storage of digital and non-digital media. Include how the agency:

A) Physically controls and securely stores information system media containing FTI.

B) Protects information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures.

Refer to Section 4.0, Secure Storage—IRC 6103(p)(4)(B), of Publication 1075 for additional secure storage requirements.

Agency SSR Response:

IRS Response:

9.3.10.5 MP-5: Media Transport

Describe how the agency protects the transport of digital and non-digital media. Include how the agency:

A) Protects and controls digital and non-digital media during transport outside of controlled areas.
B) Maintains accountability for information system media during transport outside of controlled areas.
C) Documents activities associated with the transport of information system media (the agency must use transmittals or an equivalent tracking method to ensure FTI reaches its intended destination).
D) Restricts the activities associated with the transport of information system media to authorized personnel.
E) Describe how the agency implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. (CE4)

Refer to Section 4.4, FTI in Transit, of Publication 1075 for more information on transmittals and media transport requirements.

Agency SSR Response:

IRS Response:

9.3.10.6 MP-6: Media Sanitization

Describe how the agency sanitizes media containing FTI. Include how the agency:

A) Sanitizes media containing FTI prior to disposal, release out of agency control, or release for reuse using IRS-approved sanitization techniques in accordance with applicable federal and agency standards and policies.
B) Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
C) Reviews, approves, tracks, documents, and verifies media sanitization and disposal actions. (CE1)

Additional requirements for protecting FTI during media sanitization are provided in Section 9.3.10.6, Media Sanitization (MP-6); Section 9.4.7, Media Sanitization; and Exhibit 10, Data Warehouse Security Requirements, of Publication 1075.

Agency SSR Response:

IRS Response:

9.3.11 Physical and Environmental Protection (PE)

When responding to the Physical and Environmental Protection controls, the agency should consider physical security not only for the information system, but any paper FTI, as well. Please include information about compliance with minimum protection standards (MPS) within the responses to these controls, as appropriate. For more information about MPS, refer to Publication 1075, Section 4.2.

9.3.11.1 PE-1: Physical and Environmental Protection Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.

Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.

B) Physical and environmental protection procedures to facilitate the policy and PE related security controls. Please include details regarding procedure review/update.

Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.11.2 PE-2: Physical Access Authorizations

Describe how the agency enforces physical access authorizations to the information system(s) and facilities at spaces where FTI is received, processed, stored, or transmitted. Include how the agency:

A) Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides.
B) Issues authorization credentials for facility access.
C) Reviews the access list detailing authorized facility access by individuals at least annually.
D) Removes individuals from the facility access list when access is no longer required.
E) Enforces 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. (CE1)

Note: The response for this control should encompass both access to the information system(s), as well as access to any paper FTI.

Agency SSR Response:

IRS Response:

9.3.11.3 PE-3: Physical Access Control

Describe how the agency enforces physical access controls. Include how the agency:

A) Enforces physical access authorizations at entry/exit points to facilities where the information systems that receive, process, store, or transmit FTI reside by:
   - Verifying individual access authorizations before granting access to the facility; and
   - Controlling ingress/egress to the facility using physical access control systems/devices or guards.

B) Maintains physical access audit logs for entry/exit points.

C) Provides security safeguards to control access to areas within the facility officially designated as publicly accessible.

D) Escorts visitors and monitor visitor activity.

E) Secures keys, combinations, and other physical access devices.

F) Maintains an inventory of physical access devices.

G) Changes combinations and keys when an employee who knows the combination retires, terminates employment, or transfers to another position or at least annually.

Note: The response for this control should encompass both access to the information system(s), as well as access to any paper FTI.

Agency SSR Response:

IRS Response:

9.3.11.4 PE-4: Access Control for Transmission Medium

Describe how the agency controls physical access to information system distribution and transmission lines within agency facilities.

Agency SSR Response:

IRS Response:

9.3.11.5 PE-5: Access Control for Output Devices

Describe how the agency controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output. Examples of information system output devices are: monitors, printers, copiers, scanners, fax machines, and audio devices.

Agency SSR Response:

IRS Response:

9.3.11.6 PE-6: Monitoring Physical Access

Describe how the agency monitors physical access. Include how the agency:

A) Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents. Include how the agency.

B) Reviews physical access logs.

Per Publication 1075, the agency must review physical access logs annually.

C) Coordinates results of reviews and investigations with the agency incident response capability.

D) Monitors physical intrusion alarms and surveillance equipment. (CE1)

Note: The response for this control should encompass both access to the information system(s), as well as access to any paper FTI.

Agency SSR Response:

IRS Response:

9.3.11.7 PE-8: Visitor Access Records

Describe how the agency controls access to visitors. Include how the agency:

A) Maintains visitor access records to the facility where the information system resides.

B) Document the frequency in which visitor access records are reviewed.

Per Publication 1075, the agency must review visitor access records at least annually.

Refer to Section 4.3, *Restricted Area Access*, of Publication 1075 for visitor access (AAL) requirements.

Note: The response for this control should encompass both access to the information system(s), as well as access to any paper FTI.

Agency SSR Response:

IRS Response:

9.3.11.8 PE-16: Delivery and Removal

Describe how the agency authorizes, monitors, and controls information system components entering and exiting the facility. Document how the agency maintains records of those items.

Agency SSR Response:

IRS Response:

9.3.11.9 PE-17: Alternate Work Site

Describe how the agency manages and controls alternate work sites. Include how the agency:

A) Employs IRS Office of Safeguards requirements at alternate work sites.
B) Assesses, as feasible, the effectiveness of security controls at alternate work sites.
C) Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Note: Alternate work sites may include, for example, government facilities or private residences of employees. Refer to Section 4.7: Telework Locations, of Publication 1075 for additional requirements.

Agency SSR Response:

IRS Response:

9.3.11.10 PE-18: Location of Information System Components

Describe how the agency positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Refer to Section 4.3: *Restricted Area Access*, and Section 4.5: Physical Security of Computers, Electronic, and Removable Media, of Publication 1075 for additional information.

Agency SSR Response:

IRS Response:

9.3.12 Planning (PL)

9.3.12.1 PL-1: Security Planning Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.
   Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.

B) Security planning procedures to facilitate the policy and PL related security controls. Please include details regarding procedure review/update.
   Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.12.2 PL-2: System Security Plan

Describe how the agency develops and approves an accurate System Security Plan (SSP). Please note, the agency SSR satisfies this requirement (Section 7.0, Reporting Requirements—6103(p)(4)(E), of Publication 1075). Describe how the agency:

A) Develops an SSP (or SSR) that:
   - Is consistent with the agency's safeguarding requirements;
   - Explicitly defines the 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;
   - Includes any relevant overlays, if applicable;
   - Documents the security controls in place or planned for meeting those requirements, including a rationale for the tailoring and supplementation decisions; and
   - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

B) Distributes copies of the SSP (or SSR) and communicates subsequent changes to designated agency officials and the IRS Office of Safeguards.

C) Reviews the SSP (or SSR).
   Per Publication 1075, SSPs (and the SSR) should be reviewed on at least an annual basis.

D) Updates the SSP (or SSR) to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

E) Protects the SSP (or SSR) from unauthorized disclosure and modification.

Agency SSR Response:

IRS Response:

9.3.12.3 PL-4: Rules of Behavior

Describe how the agency establishes and maintains a rules of behavior for accessing FTI and/or using information systems containing FTI. Describe how the agency:

A) Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.
B) Receives 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.
C) Reviews and updates the rule of behavior.
D) Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.
E) Includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting agency information on public websites. (CE1)

Note: The Office of Safeguards prohibits sharing FTI using any social media/networking sites.

Agency SSR Response:

IRS Response:

9.3.13 Personnel Security (PS)

9.3.13.1 PS-1: Personnel Security Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.
Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.
B) Personnel security procedures to facilitate the policy and PS related security controls. Please include details regarding procedure review/update.
Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.13.2 PS-2: Position Risk Designation

Describe how the agency identifies and controls risk designations for personnel with access to FTI. Include how the agency:

A) Assigns a risk designation to all agency positions.
B) Establishes screening criteria for individuals filling those positions.
C) Reviews and updates position risk designations.
Per Publication 1075, review and update position risk designations annually.

Agency SSR Response:

IRS Response:

9.3.13.3 PS-3: Personnel Screening

Describe how the agency:

A) Screens individuals prior to authorizing access to the information system.
B) Rescreens individuals according to agency-defined conditions requiring rescreening. Please define the frequency in the agency response.

Agency SSR Response:

IRS Response:

9.3.13.4 PS-4: Personnel Termination

Describe how the agency handles personnel termination at the agency. Include how the agency:

A) Disables information system access.
B) Terminates/revokes any authenticators/credentials associated with the individual.
C) Conducts exit interviews, as needed.
D) Retrieves all security-related agency information system–related property.
E) Retains access to agency information and information systems formerly controlled by the terminated individual.
F) Notifies agency personnel upon termination of the employee.

Agency SSR Response:

IRS Response:

9.3.13.5 PS-5: Personnel Transfer

Describe how the agency handles personnel transfer at the agency. Include how the agency:

A) Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the agency.
B) Initiates transfer or reassignment actions following the formal transfer action.
C) Modifies access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer.
D) Notifies designated agency personnel, as required.

Agency SSR Response:

IRS Response:

9.3.13.6 PS-6: Access Agreements

Describe how the agency acknowledges and authorizes access to FTI (prior to gaining access). Describe how the agency:

A) Develops and documents access agreements for agency information systems.
B) Reviews and updates the access agreements, at least annually.
C) Ensures that individuals requiring access to agency information and information systems:
- Sign appropriate access agreements prior to being granted access, and
- Re-sign access agreements to maintain access to agency information systems when access agreements have been updated or at least annually.

Agency SSR Response:

IRS Response:

9.3.13.7 PS-7: Third-Party Personnel Security

Describe how the agency manages third-party personnel security requirements. Include how the agency:

A) Establishes personnel security requirements, including security roles and responsibilities for third-party providers.
B) Requires third-party providers to comply with personnel security policies and procedures established by the agency.
C) Documents personnel security requirements.
D) Requires 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.
E) Monitors provider compliance.

Agency SSR Response:

IRS Response:

9.3.13.8 PS-8: Personnel Sanctions

Describe how the agency manages personnel sanctions. Include how the agency:

A) Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures.
B) Notifies designated agency personnel when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Agency SSR Response:

IRS Response:

9.3.14 Risk Assessment (RA)

9.3.14.1 RA-1: Risk Assessment Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.
   Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.
B) Risk assessment procedures to facilitate the policy and RA related security controls. Please include details regarding procedure review/update.
   Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.14.2 RA-3: Risk Assessment

Describe how the agency conducts regular risk assessments against the information systems and operating environments receiving, storing, processing, and/or transmitting FTI. Include how the agency:

A) Conducts an assessment 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.
B) Documents risk assessment results in a risk assessment report.
C) Reviews risk assessment results at least annually.
D) Disseminates risk assessment results to designated agency officials.
E) Updates the risk assessment report at least every three years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the system.

Agency SSR Response:

IRS Response:

9.3.14.3 RA-5: Vulnerability Scanning

Describe how the agency scans for vulnerabilities in the information system and hosted applications. Include how the agency:

A) Scans for vulnerabilities using which automated tools. Define the frequency at which vulnerability scans are conducted

Per Publication 1075, the agency must scan, at a minimum, monthly for all systems and when new vulnerabilities potentially affecting the system/applications are identified and reported.

B) Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: enumerating platforms, software flaws, and improper configurations; formatting checklists and test procedures; and measuring vulnerability impact.

C) Analyzes vulnerability scan reports and results from security control assessments.

D) Remediates legitimate vulnerabilities in accordance with an assessment of risk.

E) Shares information obtained from the vulnerability scanning process and security control assessments with designated agency officials to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

F) Employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. (CE1)

Agency SSR Response:

IRS Response:

9.3.15 System and Services Acquisition (SA)

9.3.15.1 SA-1: System and Services Acquisition Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.

Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.

B) System and services acquisition procedures to facilitate the policy and SA related security controls. Please include details regarding procedure review/update.

Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.15.2 SA-2: Allocation of Resources

Describe how the agency allocates resources to ensure information security is accounted for. Include how the agency:

A) Determines information security requirements for the information system or information system service in mission/business process planning.
B) Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process.
C) Establishes a discrete line item for information security in agency programming and budgeting documentation.

Agency SSR Response:

IRS Response:

9.3.15.3 SA-3: System Development Life Cycle

Describe how the agency manages the information system using an approved System Development Life Cycle (SDLC). Include how the agency:

A) Manages the information system using an SDLC that incorporates information security considerations.
B) Defines and documents information security roles and responsibilities throughout the SDLC.
C) Identifies individuals having information security roles and responsibilities.
D) Integrates the agency information security risk management process into SDLC activities.

Agency SSR Response:

IRS Response:

9.3.15.4 SA-4: Acquisition Process

Describe how the agency accounts for information system requirements throughout the acquisition process.

A) Describe how the agency includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and agency mission/business needs:
   - Security functional requirements; Security strength requirements; Security assurance requirements; Security-related documentation requirements; Requirements for protecting security-related documentation; Description of the information system development environment and environment in which the system is intended to operate; and Acceptance criteria.

B) When applicable, describe how the agency requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed. (CE1)

Agency SSR Response:

IRS Response:

9.3.15.5 SA-5: Information System Documentation

Describe how the agency develops and maintains information system documentation. Include how the agency:

A) Obtains administrator documentation for the information system, system component, or information system service that describes: secure configuration, installation, and operation of the system, component, or service; effective use and maintenance of security functions/mechanisms; and known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

B) Obtains user documentation for the information system, system component, or information system service that describes: user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner; and user responsibilities in maintaining the security of the system, component, or service.

C) Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent.

D) Protects documentation, as required.

E) Distributes documentation to designated agency officials.

Agency SSR Response:

IRS Response:

9.3.15.6 SA-8: System Engineering Principles

Describe how the agency applies information system security engineering principles in the specification, design, development, implementation, and modification of information systems containing, processing, or transmitting FTI.

Agency SSR Response:

IRS Response:

9.3.15.7 SA-9: External Information System Services

Describe how the agency controls and monitors external information system services. Include how the agency:

A) Requires that providers of external information system services comply with agency information security requirements and employ to include (at a minimum) security requirements contained within this publication and applicable federal laws, Executive Orders, directives, policies, regulations, standards, and established service-level agreements.
B) Defines and documents government oversight and user roles and responsibilities with regard to external information system services.
C) Monitors security control compliance by external service providers on an ongoing basis.
D) Restricts the location of information systems that receive, process, store, or transmit FTI to areas within the United States territories, embassies, or military installations. (CE5)

Note: Agencies must 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 Office of Safeguards. For notification requirements, refer to Section 7.4.5, Non-Agency-Owned Information Systems, of Publication 1075. The contract for the acquisition must contain Exhibit 7 language, as appropriate (see Section 9.3.15.4, Acquisition Process (SA-4), and Exhibit 7, Safeguarding Contract Language).

Agency SSR Response:

IRS Response:

9.3.15.8 SA-10: Developer Configuration Management

Describe how the agency requires the developer of the information system, system component, or information system service to:

A) Perform configuration management during system, component, or service development, implementation, and operation.
B) Document, manage, and control the integrity of changes to the system, component, or service.
C) Implement only agency-approved changes to the system, component, or service.
D) Document approved changes to the system, component, or service and the potential security impacts of such changes.
E) Track security flaws and flaw resolution within the system, component, or service and report findings to designated agency officials.

Agency SSR Response:

IRS Response:

9.3.15.9 SA-11: Developer Security Testing and Evaluation

Describe how the agency requires the developer of the information system, system component, or information system service to:

A) Create and implement a security assessment plan.
B) Perform security testing/evaluation.
C) Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation.
D) Implement a verifiable flaw remediation process.
E) Correct flaws identified during security testing/evaluation.

Agency SSR Response:

IRS Response:

9.3.15.10 SA-22: Unsupported System Components

Describe how the agency replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer.

Agency SSR Response:

IRS Response:

9.3.16 System and Communications Protection (SC)

9.3.16.1 SC-1: System and Communications Protection Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.

Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.

B) System and communications protection procedures to facilitate the policy and SC related security controls. Please include details regarding procedure review/update.

Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.16.2 SC-2: Application Partitioning

Describe how the agency separates user functionality (including user interface services) from information system management functionality.

Agency SSR Response:

IRS Response:

9.3.16.3 SC-4: Information In Shared Resources

Describe how the agency prevents unauthorized and unintended information transfer via shared system resources.

Agency SSR Response:

IRS Response:

9.3.16.4 SC-5: Denial of Service Protection

Describe how the agency protects against or limit the effects of denial of service attacks.

Note: Refer to NIST SP 800-61 R2, Computer Security Incident Handling Guide, for additional information on denial of service.

Agency SSR Response:

IRS Response:

9.3.16.5 SC-7: Boundary Protection

Describe how the agency protects the network boundary hosting FTI. Include how the agency:

A) Monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

B) Implements sub-networks for publicly accessible system components that are physically and logically separated from internal agency networks.

C) Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with agency security architecture requirements.

D) Limits the number of external network connections to the information system. (CE3)

E) Document how the agency:

- Implements a secure managed interface for each external telecommunication service;
- Establishes a traffic flow policy for each managed interface;
- Protects the confidentiality and integrity of the information being transmitted across each interface;
- Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need, and accept the associated risk;
- Reviews exceptions to the traffic flow policy at a minimum annually, and remove exceptions that are no longer supported by an explicit mission/business need. (CE4)

F) Describe if, and how the agency manages interfaces to deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). (CE5)

G) Describe how the agency, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the information system and connecting via some other connection to resources in external networks. (CE7)

Note: Refer to Section 9.4.10, Network Protections, of Publication 1075 for additional requirements for protecting FTI on networks.

Agency SSR Response:

IRS Response:

9.3.16.6 SC-8: Transmission Confidentiality and Integrity

Describe how the agency ensures information systems that receive, process, store, or transmit FTI are encrypted. Include how the agency:

A) Protects the confidentiality and integrity of transmitted information.
B) Implements cryptographic mechanisms to prevent unauthorized disclosure of FTI and detect changes to information during transmission across the wide area network (WAN) and within the local area network (LAN). (CE1)

Note: If encryption is not used, to reduce the risk of unauthorized access to FTI, the agency must use physical means (e.g., by employing protected physical distribution systems) to ensure that FTI is not accessible to unauthorized users. The agency must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized agency personnel. Network monitoring capabilities must be implemented to detect and monitor for suspicious network traffic. For physical security protections of transmission medium, Refer to Section 9.3.11.4, Access Control for Transmission Medium (PE-4), of Publication 1075.

This control applies 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).

Agency SSR Response:

IRS Response:

9.3.16.7 SC-10: Network Disconnect

Describe how the agency terminates the network connection associated with a communications session at the end of the session or after a predefine period of user inactivity.

Per Publication 1075, the agency must terminate network connections associated with communications session at the end of the session of after 30 minutes of inactivity.

Note: This control addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect) in contrast to user-initiated logical sessions in AC-12.

Agency SSR Response:

IRS Response:

9.3.16.8 SC-12: Cryptographic Key Establishment and Management

Describe how the agency establishes and manages cryptographic keys for required cryptography employed within the information system.

Note: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures.

Agency SSR Response:

IRS Response:

9.3.16.9 SC-13: Cryptographic Protection

Describe how the agency implements cryptographic modules in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Agency SSR Response:

IRS Response:

9.3.16.10 SC-15: Collaborative Computing Devices

Describe how the agency manages collaborative computing devices. Include how the agency:

A) Prohibits remote activation of collaborative computing devices.
B) Provides an explicit indication of use to users physically present at the devices.

Note: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

Agency SSR Response:

IRS Response:

9.3.16.11 SC-17: Public Key Infrastructure Certificates

Describe how the agency issues public key infrastructure certificates or obtains public key infrastructure certificates from an approved service provider.

Agency SSR Response:

IRS Response:

9.3.16.12 SC-18: Mobile Code

Describe how the agency regulates the use of mobile code throughout the environment. Include how the agency:

A) Defines acceptable and unacceptable mobile code and mobile code technologies.
B) Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.
C) Authorizes, monitors, and controls the use of mobile code within the information system.

Note: Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript, which are common installations on most end user workstations. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., tablet computers and smartphones).

Agency SSR Response:

IRS Response:

9.3.16.13 SC-19: Voice Over Internet Protocol

Describe how the agency controls Voice Over Internet Protocol (VoIP) technologies. Include how the agency:

A) Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously.
B) Authorizes, monitors, and controls the use of VoIP within the information system.

Note: Additional requirements for protecting FTI transmitted by VoIP systems are provided in Section 9.4.15, VoIP Systems, of Publication 1075.

Agency SSR Response:

IRS Response:

9.3.16.14 SC-23: Session Authenticity

Describe how the agency protects the authenticity of communications sessions.

Note: 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.

Agency SSR Response:

IRS Response:

9.3.16.15 SC-28: Protection of Information at Rest

Describe how the agency protects the confidentiality and integrity of FTI at rest. Include how the agency:

A) Protects the confidentiality and integrity of information at rest when located on a secondary (non-mobile) storage device (e.g., disk drive, tape drive) with cryptography mechanisms.
B) Encrypts FTI stored on deployed user workstations, in non-volatile storage, with FIPS-validated or National Security Agency (NSA)-approved encryption during storage (regardless of location) except when no approved encryption technology solution is available that addresses the specific technology.
C) Encrypts mobile devices at rest.

Note: Refer to Section 9.3.1.14, Access Control for Mobile Devices (AC-19), and Section 9.4.8, Mobile Devices, of Publication 1075 for additional information.

Agencies may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms, file share scanning, and integrity protection. Agencies may also employ other security controls, including, for example – 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.

Agency SSR Response:

IRS Response:

9.3.17 System and Information Integrity (SI)

9.3.17.1 SI-1: System and Information Integrity Policy and Procedures

Describe how the agency maintains and disseminates to designated agency officials:

A) A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Please include details regarding policy review/update.
   Per Publication 1075, the agency must review policies, and update as necessary: every three years or if there is a significant change.
B) System and information integrity procedures to facilitate the policy and SI related security controls. Please include details regarding procedure review/update.
   Per Publication 1075, the agency must review procedures, and update as necessary: annually.

Agency SSR Response:

IRS Response:

9.3.17.2 SI-2: Flaw Remediation

Describe how the agency handles flaw remediation for information systems and system components containing, processing, or transmitting FTI. Describe how the agency:

A) Identifies, reports, and corrects information system flaws.
B) Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
C) Installs security-relevant software and firmware updates based on severity and associated risk to the confidentiality of FTI.
D) Incorporates flaw remediation into the agency configuration management process.
E) Centrally manages the flaw remediation process. (CE1)

Note: Security-relevant software updates include, for example, patches, service packs, hot fixes, and antivirus signatures.

Agency SSR Response:

IRS Response:

9.3.17.3 SI-3: Malicious Code Protection

Describe how the agency applies malicious code protection mechanisms, this includes: antivirus software and antimalware and intrusion detection systems. Describe how the agency:

A) Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
B) Updates malicious code protection mechanisms whenever new releases are available in accordance with agency configuration management policy and procedures.
C) Configures malicious code protection mechanisms to:
   - Perform periodic scans of the information system weekly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with agency security policy.
   - Either block or quarantine malicious code and send an alert to the administrator in response to malicious code detection.
D) Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
E) Centrally manages malicious code protection mechanisms. (CE1)
F) Automatically updates malicious code protection mechanisms. (CE2)

Agency SSR Response:

IRS Response:

9.3.17.4 SI-4: Information System Monitoring

Describe how the agency monitors the information system and hosting network. Include how the agency:

A) Monitors the information system to detect: attacks and indicators of potential attacks; and unauthorized local, network, and remote connections.
B) Identifies unauthorized use of the information system.
C) Deploys monitoring devices: (i) strategically within the information system to collect agency-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the agency.
D) Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
E) Heightens the level of information system monitoring activity whenever there is an indication of increased risk to agency operations and assets, individuals, other organizations, or the nation, based on law enforcement information, intelligence information, or other credible sources of information.
F) Provides information system monitoring information to designated agency officials (as needed).
G) Analyzes outbound communications traffic at the external boundary of the information system and selected interior points within the network (e.g., sub-networks, subsystems) to discover anomalies.
H) Employs automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications. (CE11)
I) Implements host-based monitoring mechanisms (e.g., Host intrusion prevention system (HIPS)) on information systems that receive, process, store, or transmit FTI. (CE23)
J) Configures information systems to monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions. (CE4)
K) Configures information systems to alert designated agency officials when indications of compromise or potential compromise occur. (CE5)
L) Configures information systems to notify designated agency officials of detected suspicious events and take necessary actions to address suspicious events. (CE7)

Agency SSR Response:

IRS Response:

9.3.17.5 SI-5: Security Alerts, Advisories, and Directives

Describe how the agency utilizes information provided from security alerts, advisories, and directives. Include how the agency:

A) Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis.
B) Generates internal security alerts, advisories, and directives as deemed necessary.
C) Disseminates security alerts, advisories, and directives to designated agency officials.
D) Implements security directives in accordance with established time frames or notify the issuing agency of the degree of noncompliance.

Agency SSR Response:

IRS Response:

9.3.17.6 SI-8: Spam Protection

Describe how the agency:

A) Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.
B) Updates spam protection mechanisms when new releases are available in accordance with agency configuration management policy and procedures.

Agency SSR Response:

IRS Response:

9.3.17.7 SI-10: Information Input Validation

Describe how the agency checks the validity and accuracy of information system inputs.

Agency SSR Response:

IRS Response:

9.3.17.8 SI-11: Error Handling

Describe how the agency:

A) Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

B) Reveals error messages only to designated agency officials.

Agency SSR Response:

IRS Response:

9.3.17.9 SI-12: Information Handling and Retention

Describe how the agency handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Agency SSR Response:

IRS Response:

9.3.17.10 SI-16: Memory Protection

Describe how the agency implements safeguards to protect its memory from unauthorized code execution.

Note: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced, with hardware providing the greater strength of mechanism.

Agency SSR Response:

IRS Response:

9.3.18 Program Management (PM)

9.3.18.1 PM-2: Senior Information Security Officer

Describe how the agency appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an agency-wide information security program.

Note: The security officer described in this control is an agency official. This official is the senior information security officer. Agencies may also refer to this official as the senior information security officer or chief information security officer.

Agency SSR Response:

IRS Response:

9.4.1 Cloud Computing Environments

9.4.1.1 Cloud Computing Requirements

If the agency employs a cloud computing environment, describe how the agency meets the following requirements:

A) Notification Requirement: The agency must notify the Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment.

B) Data Isolation: Software, data, and services that receive, process, store, or transmit FTI must be isolated within the cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications.

C) SLA: The agency must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled, and accessed inside the cloud through a legally binding contract or SLA with its third-party cloud provider.

D) Data Encryption in Transit: FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate using the FIPS 140-2 compliant module. This requirement must be included in the SLA.

E) Data Encryption at Rest: FTI may need to be encrypted while at rest in the cloud, depending upon the security protocols inherent in the cloud. If the cloud environment cannot appropriately isolate FTI, encryption is a potential compensating control. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant and operate using the FIPS 140-2 compliant module. This requirement must be included in the SLA, if applicable.

F) Persistence of Data in Relieved Assets: Storage devices where FTI has resided must be securely sanitized or destroyed using methods acceptable by NSA and Central Security Service (CSS). This requirement must be included in the SLA.

G) Risk Assessment: The agency must conduct an annual assessment of the security controls in place on all information systems used for receiving, processing, storing, or transmitting FTI. For the annual assessment immediately prior to implementation of the cloud environment and each annual risk assessment (or update to an existing risk assessment) thereafter, the agency must include the cloud environment. The Office of Safeguards will evaluate the risk assessment as part of the notification requirement in Requirement A.

H) Security Control Implementation: Customer-defined security controls must be identified, documented, and implemented. The customer-defined security controls, as implemented, must comply with requirements in this publication.

Agency SSR Response:

IRS Response:

9.4.2 Data Warehouse

9.4.2.1 Data Warehouse Requirements Does the agency store or process FTI in a data warehouse environment(s)?	☐ Yes ☐ No
If Yes, has the agency provided the required notification to the Office of Safeguards?	☐ Yes ☐ No
If Yes, has the agency incorporated a discussion of the data warehouse controls in this SSR?	☐ Yes ☐ No

9.4.3 Email Communications

Describe whether FTI is permitted to be sent via email. If FTI is prohibited from inclusion within emails or email attachments, describe how the agency documents and distributes such a policy.

If FTI is allowed to be included within emails or email attachments, describe how the agency has implemented the following:

A) Policies and procedures must be implemented to ensure FTI is properly protected and secured when being transmitted via email.
B) Mail servers and clients must be securely configured according to the requirements within this publication to protect the confidentially of FTI transmitted in the email system.
C) The network infrastructure must be securely configured according to the requirements within this publication to block unauthorized traffic, limit security vulnerabilities, and provide an additional security layer to an agency's mail servers and clients.
D) Emails that contain FTI should be properly labeled (e.g., email subject contains "FTI") to ensure that the recipient is aware that the message content contains FTI.
E) Audit logging must be implemented to properly track all email that contains FTI.
F) Email transmissions that contain FTI must be encrypted using a FIPS 140-2 validated mechanism.
G) Malware protection must be implemented at one or more points within the email delivery process to protect against viruses, worms, and other forms of malware.

Agency SSR Response:

IRS Response:

9.4.4 Fax Equipment

Describe whether FTI is permitted to be sent via fax. If FTI is prohibited from inclusion within fax communications, describe how the agency documents and distributes such a policy.

If FTI is allowed to be included within fax communications, describe how the agency has implemented the following:

A) Have a trusted staff member at both the sending and receiving fax machines.
B) Accurately maintain broadcast lists and other preset numbers of frequent recipients of FTI.
C) Place fax machines in a secured area.
D) Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes:
   - A notification of the sensitivity of the data and the need for protection; and
   - A notice to unintended recipients to telephone the sender—collect, if necessary—to report the disclosure and confirm destruction of the information.

Agency SSR Response:

IRS Response:

9.4.5 Integrated Voice Response Systems

Identify whether the agency provides FTI over the telephone to a customer via an Integrated Voice Response (IVR) system. If FTI has implemented an IVR, describe how the agency has implemented the following:

A) The LAN segment where the IVR system resides is firewalled to prevent direct access from the Internet to the IVR system.
B) The operating system and associated software for each system within the architecture that receives, processes, stores, or transmits FTI to an external customer through the IVR is hardened in accordance with the requirements in this publication and is subject to frequent vulnerability testing.
C) Independent security testing must be conducted on the IVR system prior to implementation.
D) Access to FTI via the IVR system requires a strong identity verification process. The authentication must use a minimum of two pieces of information although more than two are recommended to verify the identity. One of the authentication elements must be a shared secret only known to the parties involved and issued by the agency directly to the customer. Examples of shared secrets include a unique username, PIN number, password, or pass phrase issued by the agency to the customer through a secure mechanism. Case number does not meet the standard as a shared secret because that case number is likely shown on all documents the customer receives and does not provide assurance that it is only known to the parties involved in the communication.

Agency SSR Response:

IRS Response:

9.4.6 Live Data Testing

Does the agency use live FTI in a test environment(s)?	☐ Yes ☐ No If Yes, briefly describe:
If Yes, has the agency provided the required notification to the Office of Safeguards?	☐ Yes ☐ No
If Yes, has the agency incorporated a discussion of the test environment controls in this SSR?	☐ Yes ☐ No

9.4.7 Media Sanitization

See 9.3.10.6 MP-6: Media Sanitization

9.4.8 Mobile Devices

See 9.3.1.14 AC-19: Access Control for Mobile Devices

9.4.9 Multi-Functional Devices

Describe whether multi-functional devices (MFD) are permitted for the processing of FTI. If FTI is prohibited from such devices, describe how the agency documents and distributes such a policy.

If the agency permits the use of MFDs to process FTI, describe how the agency has implemented the following:

A) The agency should have a current security policy in place for secure configuration and operation of the MFD.
B) Least functionality controls that must be in place that include disabling all unneeded network protocols, services, and assigning a dedicated static IP address to the MFD.
C) Strong security controls should be incorporated into the MFD's management and administration.
D) MFD access enforcement controls must be configured correctly, including access controls for file shares, administrator and non-administrator privileges, and document retention functions.
E) The MFD should be locked with a mechanism to prevent physical access to the hard disk.
F) The MFD firmware should be up to date with the most current firmware available and should be currently supported by the vendor.
G) The MFD and its print spoolers have auditing enabled, including auditing of user access and fax logs (if fax is enabled), and audit logs should be collected and reviewed by a security administrator.
H) All FTI data in transit should be encrypted when moving across a WAN and within the LAN.
I) Disposal of all MFD hardware follows media sanitization and disposal procedure requirements (see Section 9.3.10.6, Media Sanitization (MP-6), and Section 9.4.7, Media Sanitization).

Agency SSR Response:

IRS Response:

9.4.11 Storage Area Networks

Describe whether Storage Area Networks (SAN) are permitted for the storage and processing of FTI. If FTI is prohibited from such devices, describe how the agency documents and distributes such a policy.

If the agency permits the use of SANs to process FTI, describe how the agency has implemented the following:

A) FTI must be segregated from other agency data within the SAN environment.
B) Access controls must be implemented and strictly enforced for all SAN components to limit access to disks containing FTI to authorized users.
C) Fibre channel devices must be configured to authenticate other device with which they communicate in the SAN and authenticate administrator connections.
D) FTI must be encrypted while in transit within the SAN environment. SAN management traffic must also be encrypted for SAN components.
E) SAN components must be physically protected in accordance with the minimum protection standards for physical security described in Section 4.0, Secure Storage—IRC 6103(p)(4)(B).
F) All components of the SAN that receive, process, store, or transmit FTI must be hardened in accordance with the requirements in Publication 1075 (see SAN SCSEM available on the Office of Safeguards website).
G) SAN components must maintain an audit trail and review it on a regular basis to track access to FTI in the SAN environment.

Agency SSR Response:

IRS Response:

9.4.14 Virtualization Environments

Does the agency use virtual environment(s) to process FTI?	☐ Yes ☐ No If Yes, briefly describe:
If Yes, has the agency provided the required notification to the Office of Safeguards?	☐ Yes ☐ No
If Yes, has the agency incorporated a discussion of the virtual environment controls in this SSR?	☐ Yes ☐ No

9.4.15 VoIP Systems

Describe whether VoIP networks are used to provide FTI to a customer. If the agency does employ a VoIP implementation, describe how the agency has implemented the following:

A) VoIP traffic that contains FTI should be segmented off from non-VoIP traffic through segmentation. If complete segmentation is not feasible, the agency must have compensating controls in place and properly applied that restrict access to VoIP traffic that contains FTI.
B) When FTI is in transit across the network (either Internet or state agency's network), the VoIP traffic must be encrypted using a NIST-approved method operating in a NIST-approved mode.
C) VoIP network hardware (servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in Section 4.0, Secure Storage—IRC 6103(p)(4)(B).
D) Each system within the agency's network that transmits FTI to an external customer through the VoIP network is hardened in accordance with the requirements in this publication and is subject to frequent vulnerability testing.
E) VoIP-ready firewalls must be used to filter VoIP traffic on the network.
F) Security testing must be conducted on the VoIP system prior to implementation with FTI and annually thereafter.
G) VoIP phones must be logically protected, and agencies must be able to track and audit all FTI-applicable conversations and access.

Agency SSR Response:

IRS Response:

9.4.16 Web-Based Systems

Describe whether an external Web-based system or website is used to provide FTI to a customer. If the agency does employ a Web-based system, describe how the agency has implemented the following:

A) The system architecture is configured as a three-tier architecture with physically separate systems that provide layered security of the FTI, and access to the database through the application is limited.
B) Each system within the architecture that receives, processes, stores, or transmits FTI to an external customer through the Web-based system or website is hardened in accordance with the requirements in this publication and is subject to frequent vulnerability testing.
C) Access to FTI via the Web-based system or website requires a strong identity verification process. The authentication must use a minimum of two pieces of information although more than two is recommended to verify the identity. One of the authentication elements must be a shared secret only known to the parties involved and issued by the agency directly to the customer. Examples of shared secrets include a unique username, PIN number, password, or pass phrase issued by the agency to the customer through a secure mechanism. Case number does not meet the standard as a shared secret because that case number is likely shown on all documents the customer receives and does not provide assurance that it is only known to the parties involved in the communication.

Agency SSR Response:

IRS Response:

9.4.17 Web Browser

Describe whether a web browser is used to access FTI. If the agency does employ a web browser to access FTI, describe how the agency has implemented the following:

A) Private browsing must be enabled on the Web browser and configured to delete temporary files and cookies upon exiting the session.
B) Install vendor-specified security patches and hot fixes regularly for the Web browser, add-ons, and Java.
C) Security enhancements, such as pop-up blocker and content filtering, must be enabled on the Web browser.
D) Configure the designated Web browser in accordance to the principle of least functionality and disable items, such as third-party add-ons.
E) Deploy a Web gateway to inspect Web traffic and protect the user workstation from direct exposure to the Internet.
F) FTI transmission within the agency's internal network must be encrypted using a cryptographic module that is FIPS 140-2 validated.
G) Determine the business use of Java and approve the use of Java if is required for core business functions.

Agency SSR Response:

IRS Response:

9.4.18 Wireless Networks

Describe whether a wireless network is used to access FTI. If the agency does employ a wireless network to access FTI, describe how the agency has implemented the following:

A) The agency should have WLAN management controls that include security policies and procedures, a complete inventory of all wireless network components, and standardized security configurations for all components.
B) WLAN hardware (access points, servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in Section 4.0, Secure Storage—IRC 6103(p)(4)(B).
C) Each system within the agency's network that transmits FTI through the WLAN is hardened in accordance with the requirements in this publication.
D) The WLAN is architected to provide logical separation between WLANs with different security profiles and from the wired LAN.
E) WLAN infrastructure that receives, processes, stores, or transmits FTI must comply with the Institute of Electrical and Electronic Engineers 802.11i wireless security standard and perform mutual authentication for all access to FTI via 802.1X and extensible authentication protocol.
F) Vulnerability scanning should be conducted as part of periodic technical security assessments for the organization's WLAN.
G) Wireless intrusion detection is deployed to monitor for unauthorized access, and security event logging is enabled on WLAN components in accordance with Section 9.3.3, Audit and Accountability.
H) Disposal of all WLAN hardware follows media sanitization and disposal procedures in Section 9.3.10.6, Media Sanitization (MP-6), and Section 9.4.7, Media Sanitization.

Agency SSR Response:

IRS Response:

10. Disclosure Awareness

Describe the agency's formal disclosure awareness program. Provide procedure information for initial and annual certification. Provide a sample copy of training materials presented to employees and contractors.

As part of the awareness training and certification program employees and contractors must be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and Exhibit 5, IRC Sec. 7213 Unauthorized Disclosure of Information).

Note: Each agency receiving FTI must have an awareness program that annually notifies all employees having access to FTI of the confidentiality provisions of the IRC, a definition of what returns and what return information is, and the civil and criminal sanctions for unauthorized inspection or disclosure.

Attachments: Sample copy of training materials (required if changes have been made)

Publication 1075: Section 6.3

Agency SSR Response:

IRS Response: