CALIFORNIA DEPARTMENT OF CHILD SUPPORT SERVICES
P.O. Box 419064, Rancho Cordova, CA 95741-9064

February 19, 2016

Reason for this Transmittal

[X] State Law or Regulation Change
[X] Federal Law or Regulation Change
[ ] Court Order or Settlement Change
[ ] Clarification requested by One or More Counties
[ ] Initiated by DCSS

CSS Letter: 16-03

ALL IV-D DIRECTORS
ALL COUNTY ADMINISTRATIVE OFFICERS
ALL BOARDS OF SUPERVISORS

SUBJECT: SAFEGUARDS SECURITY REPORT, FORMERLY CALLED SAFEGUARDS ACTIVITY REPORT

The purpose of this letter is to provide the local child support agencies (LCSAs) with direction regarding the new Internal Revenue Service (IRS) Safeguards Security Report (SSR), formerly called the Safeguard Activity Report. This letter supersedes CSS letter 09-01, Annual Safeguard Activity Report.

Pursuant to Internal Revenue Code Section 6103, recipient agencies that legally receive federal tax information (FTI) directly from either the IRS or from secondary sources (e.g. Social Security Administration, Office of Child Support Enforcement), 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.*

Provided with this letter are:

- Safeguards Security Report (SSR) template – Green text boxes within the SSR template provide additional information to facilitate the completion of the SSR.
- SSR Training PowerPoint – The training slides include step by step instructions to complete the SSR.
- ISO File Library Instructions – A step-by-step guide with instructions to use the easy and secure application. The ISO File Library is located on the LCSA Secure Website and is used to ensure secure document exchange between the Information Security Office (ISO) and the LCSA.

The IRS requires each LCSA to complete the IRS SSR annually. The SSR is a comprehensive report of the security controls in place to safeguard FTI. The annual SSR reporting period is February 1 through January 31 of the following year (i.e. February 1, 2016 through January 31, 2017). LCSAs must provide responses directly in the body of the SSR template and then securely submit the SSR annually to the DCSS Information Security Office via the ISO File Library application on or before January 31 of each year.

All LCSAs are responsible for completing SSR Sections 1through 8. These sections address the administrative and physical safeguard activities. Option 2 and 3 LCSAs must also complete SSR Section 9, Information Security Controls. Option 1 LCSAs are exempt from completing Section 9, because the state provides its information technology (IT) network and support resources, and is responsible for all technical security safeguards.

Section 9 of the SSR addresses the security controls in place to information systems that receive, process, store, or transmit child support information, including FTI. We encourage Option 2 and 3 staff to work with their individual county IT agency representatives to complete Section 9. If a security control is not applicable to the agency, provide justification or the compensating security measures the agency has implemented to ensure the confidentiality and integrity of child support data.

Please do not submit the completed SSR to the IRS. The ISO will incorporate responses into one SSR document for submittal to the IRS. If you have any questions or concerns regarding this information or need assistance in completing the SSR template, please contact the DCSS ISO at (916) 464-5045.

Sincerely,

O/S

JOHN CLEVELAND
Chief Information Security Officer
Technology Services Department

Attachments: SSR Template (LCSA Version)
SSR Training (Slides)
ISO File Library Instructions

Internal Revenue Service (IRS)
Office of Safeguards

Safeguards Security Report (SSR)

[Agency Name]

[Reporting Year]

NOTE: The DCSS Information Security Office (ISO) has provided additional clarification and instruction throughout the SSR to assist in completing the document. Please feel free to also contact the ISO mailbox; info.security@dcss.ca.gov for any questions.

Report Information			
Agency Name:	[Insert agency name]	**Agency Address:**	
DCSS ISO Reviewer:	[Leave blank]	**Date Submitted:**	[Insert date of SSR submission to DCSS ISO]

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 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 DCSS ISO at info.security@dcss.ca.gov mailbox timely and cooperate with the investigations, 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

SSR must be signed by agency head on an annual basis, and prior to SSR submission. NOTE: a formal cover letter is no longer required.

2 Agency Information	
The questions in Section 2, Agency Information must be updated annually.	
1.1 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.	
1.2 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. Include LCSA security manage/privacy officer or disclosure officer – would be the primary designated contact to work with on safeguard activities.	
1.3 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. Include Option 2 and 3 LCSA, IT security manager/officer, responsible for the implementation of county safeguard procedures and compliance with Publication 1075 security controls.	

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 of the SSR. If documentation is requested, please provide as an attachment.

3.1.1 FTI Data Received

Summarize the FTI received during the reporting period (both electronic and paper). Include the source, type of file or extract, and volume of records received.

Note: *A summary from the record keeping logs required in Publication 1075 Section 3 for electronic and paper data would meet this requirement.*

Publication 1075: Section 3.0

The agency must establish a tracking system to identify and track the location of electronic and non-electronic FTI.
A log of FTI received may include tracking elements such as:

- Taxpayer name or other identifying number
- Tax years(s)
- Type of information (e.g. revenue report/Form 1040)
- The reason for the request
- Date received
- Exact location of the FTI
- Who has had access to the FTI data
- If disposed of, the date and method of disposition

FTI must not be maintained in the log if downloaded from DCSS automated systems.

Agency SSR Response:

3.1.2 Disposal of FTI

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

Note: *A summary from the record keeping logs required in Publication 1075 Section 3 for electronic and paper data would meet this requirement.*

Publication 1075: Section 8.0

Please note this section is specific to the current reporting cycle only. Please document all FTI disposed during the agency's current reporting period.
Section 8.1 (Disposal) will be used to document agency methods, policies, and procedures of FTI disposal and will include a sample of the destruction log.

Agency SSR Response:

3.1.3 Re-disclosure of FTI Does the agency have a current (p) (2) (B) agreement(s)?	☐ Yes ☐ No
Has the agency re-disclosed FTI through a (p) (2) (B) agreement? *Publication 1075: Section 11.4* Select YES only if re-disclosure agreements are in place.	☐ Yes ☐ No If Yes, provide the agency to which FTI was provided and the number of records provided:

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 of the SSR. If documentation is requested, please provide as an attachment.

4.1 Current Period Changes

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 X:
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
Has the agency added or changed contractors with access to FTI?	☐ Yes ☐ No
If Yes, has the agency submitted the appropriate 45 day notifications to the Office of Safeguards? *Publication 1075: Section 7.4.3* If YES, also provide update in Section 5.2.	☐ Yes ☐ No
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? If YES, also provide update in Section 9.2.	☐ Yes ☐ No

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? If YES, also provide update in Section 9.3.11.	☐ Yes ☐ No
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)? If YES, also provide update in Section 8.	☐ Yes ☐ No
Has the agency changed its use of FTI for the purpose of tax modeling? *Publication 1075: Section 7.4.3* Check NO. DCSS is not a state tax agency.	☐ Yes ☐ No
4.2 Planned Changes	
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. Although SSR submission is annual, please note 45 Day notifications still required throughout agency's reporting cycle.	☐ 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 is 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 Received

Provide a list of the FTI the agency receives and whether the data is received through electronic or non-electronic methods. 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.

See Publication 1075 Section 3.0

This is different from Section 3.1.1, FTI 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 is all inclusive, it can be referenced here in Section 5.1.

Agency SSR 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.*

See Publication 1075 Section 3.0

Please provide a network diagram that shows the various devices, systems and access points that are involved in the flow of FTI.

Agency SSR 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.*

Publication 1075: Section 3.0

This record keeping should include internal requests among agency employees as well as requests outside of the agency. If your process is completely paperless and no paper FTI is involved in your process, then you can refer to the system audit logging mechanisms that are in place on the various systems involved in processing FTI.

If you have any printed FTI or printed files containing FTI, then the distribution of those files must be logged and tracked.

See Pub 1075, Section 3.3 for the suggested data to capture on the log.

Agency SSR 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

NOTE: not applicable for LCSAs.

Section 7.1 will be completed by DCSS Information Security Office (ISO). DCSS ISO will describe the process for conducting internal inspections of headquarters, field offices, data center, offsite storage, and contractor sites.

Please note this is separate from a CAP (Corrective Action Plan) reporting and refers to how the agency tracks findings/vulnerabilities identified during self-assessments and through internal inspections.

Agency SSR 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.*

Publication 1075: Section 6.4

This is different from Section 3.1.2, Disposal of FTI. Please reference the procedures established by the agency for ensuring proper disposal methods are used in accordance with Pub 1075, Section 8, Disposal.

Agency SSR 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 is 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), release, review, or update date(s), and a short summary of the content of the document(s) as it relates to that control family.

This section should be completed by Option 2 and 3 LCSAs. Option 1 LCSAs are exempt from completing Section 9.

We encourage Option 2 and 3 LCSAs to work with individual county Information Technology (IT) representatives to complete Section 9 Information Security Controls. If a security control is not applicable to the agency, please provide a justification or describe the compensating security measures the agency has implemented to ensure the confidentiality and integrity of FTI.

Please contact the DCSS ISO mailbox at info.security@dcss.ca.gov for questions/clarification regarding any security control requirements.

9.1.1 Provide the name and address where the agency's IT equipment resides (e.g. data center, computer room).

This section is referring to the primary data center location, whether that is a contractor/provider or state data center site. Please include any secondary and/or disaster recovery data centers where FTI is housed.

Agency SSR 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

Please include details about the data center location. We would like to understand the environment with respect to other tenants co-located in the data center who would have personnel with physical access to systems that contain FTI.

Please include any secondary and/or disaster recovery data centers where FTI is housed.

Agency SSR 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), Cyber Fusion, Connect: Direct)

Reuse the content that was provided in Section 3 Data Flow as it relates to the IT systems and not the department or organizational units that access the data. In the agency's response, please include information system components and technologies. Describe any safeguards in place to protect FTI and describe the process from original receipt of FTI to destruction in your response.

Agency SSR 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
- Include details regarding policy review/update (every three years or if there is a significant change)

B) Access control procedures to facilitate the policy and AC related security controls
- Include details regarding policy review/update (annually)

The agency must develop and maintain access control policies and procedures. See Pub 1075, Section 9.3.1.1 (page 44) for further guidance.

Agency SSR 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 specifies authorized user accounts with access to FTI to support agency mission/business functions

B) Assigns account managers and requires approval for access to user accounts with FTI access; notifies account managers when accounts are no longer required

C) Creates, enables, modifies, disables, and removes information system accounts in accordance with documented agency account management procedures

D) Establishes conditions for group and role membership and establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group

E) Monitors the use of information system accounts with access to FTI

Publication 1075 requirement: Reviews a list of standard user accounts at least annually; and semi-annually for privileged accounts for compliance with AC policy and procedures

F) Automatically disables inactive accounts after a period of user inactivity (CE3)

Publication 1075 requirement: 120 days

If agency defined/implemented frequencies do not satisfy the Pub 1075 requirement, please include any compensating security measures the agency has implemented to ensure the confidentiality and integrity of FTI. Please see Pub 1075 Section 9.3.1.2 (pages 44-45) for further guidance.

Agency SSR 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

The information system must enforce assigned authorizations for controlling system access. Please see Pub 1075 Section 9.3.1.3 (page 45) for further guidance.

Agency SSR 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.

Flow control restrictions include keeping export-controlled information from being transmitted in the clear to the internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the internet that are not from the internal web proxy server, and limiting transfers between organizations based on data structures and content. Please see Pub 1075 Section 9.3.1.4 (page 45) for further guidance.

Agency SSR 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) Document the roles and permissions used to separate duties

C) Define information system access authorizations used to support the separation of duties for users authorized access to FTI.

The agency must ensure the information system enforces separation of duties through assigned access authorizations. See Pub 1075 Section 9.3.1.5 (page 46) for examples of Separation of Duties and for further guidance.

Agency SSR Response:

9.3.1.6 AC-6: Least Privilege

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

D) Explicitly authorizes access to FTI (CE1)

E) 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)

F) Restricts privileged accounts on the information system to a limited number of individuals with a need to perform administrative duties (CE5)

G) Audits the execution of privileged functions (CE9)

H) Prevents non-privileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures (CE10)

The information system must enforce the most restrictive access capabilities users need to perform specific tasks. See Pub 1075 Section 9.3.1.6 (page 46) for suggested model and for further guidance.

Agency SSR 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

Publication 1075 requirement: 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

Publication 1075 requirement: Automatically lock the account until released by an administrator

The information system must limit the number of consecutive unsuccessful access attempts allowed in a specific period and automatically perform a specific function (e.g. account lockout) when the maximum number of attempts is exceeded. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. See Pub 1075 Section 9.3.1.7 (page 46) for further guidance.

Agency SSR Response:

9.3.1.8 AC-8: System Use Notification

Describe how the agency displays an IRS-approved warning banner to users of information systems containing FTI. Provide the text of the warning banner. The warning banner must include:

- The system contains U.S. Government information
- Users actions are monitored and audited
- Unauthorized use of the system is prohibited
- Unauthorized use of the system is subject to criminal and civil sanctions

A) Document if the information system is publicly accessible and provide warning banner language (see Publication 1075 for publicly accessible information system requirements)
B) Identify all components (application, database, operating system, network devices) that contain the approved message
C) Document how the user acknowledges the warning banner prior to gaining system access

Publication 1075 requirement: Retain the warning banner on the screen until users acknowledge the usage conditions and take explicit actions to further access the information system

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

In addition to narrative response, please provide screenshot(s) of warning banner(s) in use at the agency for protecting information system(s) receiving, processing, storing, and/or transmitting FTI. The warning banner must also be applied at the application, database, operating system, and network devise. See Pub 1075 Section 9.3.1.8 (page 47) for further guidance.

Agency SSR 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

Publication 1075 requirement: 15 minutes

B) Document the action taken to reestablish access

Publication 1075 requirement: Retain the session lock until the user reestablishes access using established identification and authentication procedures

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information system but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. See Pub 1075 Section 9.3.1.9 (page 48) for further guidance.

Agency SSR 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.

Publication 1075 requirement: 15 minutes

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).

The information system shall automatically terminate any remote session after ten minutes of inactivity, where these systems contain child support information, containing FTI. For instances of interactive and/or batch processing, compensating controls must be implemented. See Pub 1075 Section 9.3.1.10 (page 47-48) for further guidance.

Agency SSR Response:

9.3.1.11 AC-14: Permitted Actions without Identification or Authentication

Describe how the agency identifies and documents specific user actions that can be performed on the information system without identification or 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. Include how the agency:

A) Identifies specific user actions that can be performed on the information system without identification or authentication consistent with agency missions/business functions. FTI may not be disclosed to individuals on the information system without identification and authentication. Provide supporting rationale for the user actions not requiring identification or authentication

The agency must identify and document specific user actions that can be performed on the information system without identification or authorization. Management must supervise and review the activities of the users as this relates to information system access. See Pub 1075 Section 9.3.1.11 (page 48) for further guidance.

Agency SSR Response:

9.3.1.12 AC-17: Remote Access

Describe how the agency authorizes, documents, and monitors all remote access capabilities used on the system, where these systems containing FTI. Remote access is defined as any access to an agency information system by a user communicating through an external network, for example: the Internet. Include how the agency has implemented:

A) Usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed
B) Authorization process for allowing remote access to the information system
C) Authorization process for allowing the execution of privileged commands and access to security-relevant information via remote access for compelling operational needs only (CE4)
D) Process for monitoring and controlling remote access methods (CE1)

Publication 1075 requirements:

- Remote access where FTI is accessed must be performed using multi-factor authentication
- FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore (outside the United States)
- Cryptographic mechanisms shall be implemented to protect the confidentiality and integrity of remote access sessions where FTI is transmitted over the remote connection (CE2)
- All remote accesses shall be routed through a limited number of managed network access control points (CE3)

Agencies often employ encrypted virtual private network (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. See Pub 1075 Section 9.3.1.12 (page 48-49) for further guidance.

Agency SSR 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 applies the following to further protect FTI:

A) Wireless access policies that establish usage restrictions, configuration/connection requirements, implementation guidance for wireless access, and the authorization process of wireless access to the information system
B) 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)
C) Authentication and encryption (CE1)

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

Agencies must develop and maintain policies and procedures for allowed wireless access, where these systems contain FTI. As part of the wireless access, the agency shall authorize, document, and monitor all wireless access to the information system. See Pub 1075 Section 9.3.1.13 (page 49) for further guidance.

Agency SSR 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 has implemented:

A) Mobile device policies that establish usage restrictions, configuration/connection requirements, implementation guidance for agency-controlled mobile devices, and the authorization process of connecting mobile devices to agency information systems

B) Encryption to protect the confidentiality and integrity of information on mobile devices (e.g., smartphones and laptop computers) (CE5)

C) Mobile device purging and wiping capabilities

Publication 1075 requirement: Purge/wipe 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.

Agencies must develop and maintain policies and procedures for allowed portable and mobile devices, where these systems contain FTI. As part of the wireless access, the agency shall authorize, document, and monitor all wireless access to the information system. See Pub 1075 Section 9.3.1.14 (page 49-50) for further guidance.

Agency SSR Response:

9.3.1.15 AC-20: Use of External Information Systems

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.

Agencies must develop and maintain policies and procedures for authorized individuals to access the information systems from an external system. See Pub 1075 Section 9.3.1.15 (page 50) for further guidance.

Agency SSR 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.

See Pub 1075 Section 9.3.1.16 (page 50) for further guidance.

Agency SSR 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

Publication 1075 requirement: At a minimum conduct quarterly reviews of information

See Pub 1075 Section 9.3.1.17 (page 50) for further guidance.

Agency SSR 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
   - Include details regarding policy review/update (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
   - Include details regarding policy review/update (annually)

The agency must develop and maintain awareness and training policies and procedures. See Pub 1075 Section 9.3.2.1 (page 51) for further guidance.

Agency SSR 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. 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

A) Describe the content of security awareness training

Publication 1075 requirement: Include security awareness training on recognizing and reporting potential indicators of insider threat (CE2)

The agency must ensure all information system users and managers have completed security awareness training before authorizing access to the system. See Pub 1075 Section 9.3.2.2 (page 51) for further guidance.

Agency SSR Response:

9.3.2.3 AT-3: Role Based Security Training

Describe how the agency identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides sufficient security training before authorizing access to the information system and FTI.

Publication 1075 requirement: Role based security training must be completed prior to information system access and/or to FTI, when required by information system changes, and at least annually thereafter

The agency must identify personnel with significant information system security roles and responsibilities, document those roles and responsibilities, and provide sufficient security training before authorizing access to the information system and FTI. See Pub 1075 Section 9.3.2.3 (page 52) for further guidance.

Agency SSR Response:

9.3.2.4 AT-4: Security Training Records

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

A) Define the duration in which individual training records are retained

Publication 1075 requirement: Retain individual training records for a period of five years

The agency must document and monitor individual information system security training activities including basic security awareness training and specific information system security training. See Pub 1075 Section 9.3.2.4 (page 52) for further guidance.

Agency SSR 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
   - Include details regarding policy review/update (every three years or if there is a significant change)

B) Audit and accountability procedures to facilitate the policy and AU related security controls
   - Include details regarding policy review/update (annually)

The agency must develop and maintain audit and accountability policies and procedures. See Pub 1075 Section 9.3.3.1 (page 52) for further guidance.

Agency SSR 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

Publication 1075 requirement: 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) Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents

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

Publication 1075 requirement: Review and update the audited events at a minimum, annually

Note: *Coordinate the security audit function with other agency entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events.*

The information system must generate audit records for all security-related events, including all security and system administrator accesses. See Pub 1075 Section 9.3.3.3 (page 53-54) for further guidance.

Agency SSR 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

Publication 1075 requirement: At a minimum, 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)

Security-relevant events must enable the detection of unauthorized access to FTI data. See Pub 1075 Section 9.3.3.4 (page 54) for further guidance.

Agency SSR 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.

Publication 1075 requirement: Allocate audit record storage capacity to retain audit records for the required audit retention period of seven years

Agencies must configure the information system to allocate sufficient audit record storage capacity to record all necessary auditable items. See Pub 1075 Section 9.3.3.5 (page 54) for further guidance.

Agency SSR 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)

Document different audit processing failures, and describe the methods in place for altering designated agency officials of each failure. See Pub 1075 Section 9.3.3.6 (page 54) for further guidance.

Agency SSR 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

Publication 1075 requirement: 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

Publication 1075 requirement: 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.

The agency must routinely review audit records for indications of unusual activities, suspicious activities or suspected violations, and report findings to appropriate officials for prompt resolution. See Pub 1075 Section 9.3.3.7 (page 54-55) for further guidance.

Agency SSR 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.

Publication 1075 requirement: The capability shall support on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and shall not alter the original content or time ordering of audit records

Accurate time stamping of audit records is critical for audit reduction and report generation. See Pub 1075 Section 9.3.3.8 (page 55) for further guidance.

Agency SSR 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

Publication 1075 requirement: Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT)

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

The information system shall provide date and time stamps for use in audit record generation. See Pub 1075 Section 9.3.3.9 (page 56) for further guidance.

Agency SSR Response:

9.3.3.10 AU-9: Protection of Audit Information

Describe how the agency's information system(s) protects audit information and audit tools from unauthorized access, modification, and deletion.

A) 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.

Publication 1075 requirement: System and network administrators must not have the ability to modify or delete audit log entries (CE4)

The information system protects audit information and audit tools from unauthorized access, modification, and deletion. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls. See Pub 1075 Section 9.3.3.10 (page 56) for further guidance.

Agency SSR 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.

Publication 1075 requirement: 7 years

To support audit activities, all agencies must ensure that audit information is archived for seven years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored. See Pub 1075 Section 9.3.3.11(page 56) for further guidance.

Agency SSR 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) Generates audit records with the content defined in Section 9.3.3.4 (AU-3: Content of Audit Records)
C) Allows designated agency officials to select which auditable events are to be audited by specific components of the information system.

Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit events. Please document and include if the agency employ any automated tools to facilitate this process. See Pub 1075 Section 9.3.3.12 (page 56-57) for further guidance.

Agency SSR 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.

This requirement should be accomplished through Memorandum of Understanding (MOU), Service Level Agreement (SLA), and contractual agreements. See Pub 1075 Section 9.3.3.13 (page 58) for further guidance.

Agency SSR 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
   - Include details regarding policy review/update (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
   - Include details regarding policy review/update (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 shall develop and maintain policies and procedures that address the processes used to test, validate, and authorize the security controls used to protect FTI. See Pub 1075 Section 9.3.4.1 (page 58) for further guidance.

Agency SSR 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.

Publication 1075 requirement: Assess the security controls in the information system and its environment at a minimum of an annual basis

A) Include 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) Include how the agency assesses security controls applicable to the information system and its environment
C) Include how the agency reports assessment results in a security assessment report, and provides results to the agency's Authorizing Official

The agency shall conduct an assessment of the information system security controls to ensure the controls are implemented correctly, operating as intended, and producing the desired outcome. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; (iv) ensure compliance to vulnerability mitigation procedures. See IRS Publication 1075 Section 9.3.4.2 (pages 58-59) for further guidance.

Agency SSR Response:

9.3.4.3 CA-3: System Interconnections

Describe how the agency develops and maintains Interconnection Security Agreement (ISA) for external information system connections.

A) Define the content of ISA language, including but not limited to: the interface characteristics, security requirements, nature of the information transmitted, and review schedule
   Publication 1075 requirement: Review and update the system interconnection on an annual basis
B) 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)

This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. See IRS Publication 1075 Section 9.3.4.3 (page 60) for further guidance.

Agency SSR Response:

9.3.4.4 CA-5: Plan of Action and Milestones

Describe how the agency develops and updates a Plan of Action & Milestones (POA&M) 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) Define the frequency in which the POA&M is reviewed and updated by the agency

Publication 1075 requirement: At a minimum, quarterly

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 vulnerability 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.

The agency shall develop and maintain a Plan of Actions and Milestones that identify any deficiencies related to FTI processing. See IRS Publication 1075 Section 9.3.4.4 (page 60) for further guidance.

Agency SSR 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

The agency shall undergo a security assessment and authorization every three (3) years or whenever there is a significant change to the control structure. Authorizing official must be a senior level executive that's also an owner of the FTI data. For systems processing FTI, IRS does not require third-party authorization of the security controls. The state may internally attest in writing that the security controls have been adequately implemented to protect FTI by having a senior agency official sign and approve the authorization. See IRS Publication 1075 Section 9.3.4.5 (page 60) for further guidance.

Agency SSR Response:

9.3.4.6 CA-7: Continuous Monitoring

Describe how the agency has developed an information system 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

Publication 1075 requirement: At a minimum, annually

B) Procedures for the execution of ongoing security control assessments

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.

The agency shall monitor the security controls within the information system hosting FTI to ensure that the controls are operating as intended. Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. See IRS Publication 1075 Section 9.3.4.6 (page 61) for further guidance. .

Agency SSR 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
- Include details regarding policy review/update (every three years or if there is a significant change)

B) Configuration management procedures to facilitate the policy and CM related security controls
- Include details regarding policy review/update (annually)

The agency must ensure that configuration management policy and procedures must be developed and maintained to facilitate implementing configuration management security controls. See IRS Publication 1075 Section 9.3.5.1 (page 61) for further guidance.

Agency SSR Response:

9.3.5.2 CM-2: Baseline Configuration

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

A) Include the agency's frequency of review and update of the baseline configuration of the information system (CE1)

Publication 1075 requirement: 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.

The agency must develop and maintain current baseline configuration of the information system. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. See IRS Publication 1075 Section 9.3.5.2 (page 61) for further guidance.

Agency SSR 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)

The agency must have a designated individual(s) to authorize, document and maintain control changes to the information system. Describe whether or not the agency has a formal Change Control Board.

Configuration change controls for agency information systems and components should involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. See IRS Publication 1075 Section 9.3.5.3 (page 62) for further guidance.

Agency SSR 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.

The agency must monitor changes to the information system conducting security impact analysis to determine the effects of the changes. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include; reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. See IRS Publication 1075 Section 9.3.5.4 (page 62) for further guidance.

Agency SSR 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.

The agency must approve individual access privileges and enforce physical and logical access restrictions associated with changes to the information system and generate, retain, and review records reflecting all such changes. Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. See IRS Publication 1075 Section 9.3.5.5 (page 62) for further guidance.

Agency SSR Response:

9.3.5.6 CM-6: Configuration Settings

Describe how the agency 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. Include how the agency addresses:

A) Implements the configuration settings
B) Identifies, documents, and approves any deviations from established configuration settings for information systems that receive, process, store, or transmit FTI
C) Monitor and control 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).*

The agency shall establish mandatory configuration settings for information technology products employed within the information system that (i) configures the security settings of information technology products to the most restrictive mode consistent with operational requirement; (ii) documents the configuration settings; and (iii) enforces the configuration settings in all components of the information system. See IRS Publication 1075 Section 9.3.5.6 (pages 62-63) for further guidance.

Agency SSR 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

The agency shall restrict access for change, configuration settings, and provide the least functionality necessary. Some IT component functions and services, provided by default, may not be necessary to support essential agency operations (e.g., key missions, functions). Where feasible, the agency should limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Agencies can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. See IRS Publication 1075 Section 9.3.5.7 (page 63) for further guidance.

Agency SSR Response:

9.3.5.8 CM-8: Information System Component Inventory

Describe how the agency develops and documents an inventory of information system components. The inventory shall accurately reflect the current information system; include all components that store, process, or transmit FTI; is at the level of granularity deemed necessary for tracking and reporting; and include information deemed necessary to achieve effective information system component accountability.

A) 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

Publication 1075 requirement: Update 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.

The agency shall develop and maintain a current inventory of the components of the information system and relevant ownership information. Information deemed necessary for effective accountability of information system components includes: hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include: manufacturer, device type, model, serial number, and physical location. See IRS Publication 1075 Section 9.3.5.8 (pages 63-64) for further guidance.

Agency SSR 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.

Publication 1075 requirement: 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
- Protect the CMP from unauthorized disclosure and modification

Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. See IRS Publication 1075 Section 9.3.5.9 (page 64) for further guidance.

Agency SSR Response:

9.3.5.10 CM-10: Software Usage Restrictions

Describe how the agency uses software and associated documentation in accordance with contract agreements and copyright laws. Describe how the agency addresses software usage requirements:

A) Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution

B) 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

C) Establish restrictions on the use of open source software

Publication 1075 requirement: 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)

Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on agency needs. See IRS Publication 1075 Section 9.3.5.10 (page 64) for further guidance.

Agency SSR 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

If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include; updates and security patches to existing software and downloading applications from organization-approved "app stores." Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both. See IRS Publication 1075 Section 9.3.5.11 (page 64) for further guidance.

Agency SSR 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:

C) A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
- Include details regarding policy review/update (every three years or if there is a significant change)

D) Contingency planning procedures to facilitate the policy and CP related security controls
- Include details regarding policy review/update (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 backup media or used at alternative facilities and not focused on the availability of data. Agencies must develop applicable contingencies for ensuring that FTI is available, based upon their individual risk-based approaches. 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.

The agency must develop and maintain applicable contingencies for ensuring that FTI is available, based upon their individual risk-based approaches. See IRS Publication 1075 Section 9.3.6.1 (page 65) for further guidance.

Agency SSR 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.

Publication 1075 requirements: 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 protected from unauthorized disclosure and modification
- Be reviewed at least annually; Updates shall be communicated to key contingency personnel, and shall address changes to the agency, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing

Contingency planning for information systems is part of an overall agency program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. See IRS Publication 1075 Section 9.3.6.2 (pages 65-66) for further guidance.

Agency SSR Response:

9.3.6.3 CP-3: Contingency Training

Describe how the agency tests contingency plans to determine the effectiveness of the plan and the agency's readiness to execute the plan. Describe how the contingency plan test results are reviewed, and how corrective actions are initiated (if applicable).

Publication 1075 requirement: Test the contingency plan for the information system, at a minimum annually

See IRS Publication 1075 Section 9.3.6.3 (page 66) for further guidance.

Agency SSR Response:

9.3.6.4 CP-4: Contingency Plan Testing

For Federal agencies, describe how personnel are trained in their contingency roles and responsibilities with respect to the information system.

Publication 1075 requirement: Testing shall occur prior to assuming a contingency role or responsibility, when required by information system changes, and annually thereafter

The agency must ensure that plans are tested to ensure procedures and staff personnel are able to provide recovery capabilities within established timeframes. Methods for testing include contingency plans to determine the effectiveness and to identify potential weaknesses. See IRS Publication 1075 Section 9.3.6.4 (page 66) for further guidance.

Agency SSR Response:

9.3.6.5 CP-6: Alternate Storage Site

Describe how the agency identifies alternate storage sites and initiates necessary agreements to permit the secure storage and retrieval of information system and FTI backups. Ensure the alternate storage site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103.

The agency must identify alternate storage sites and initiate necessary agreements to permit the secure storage of information system and FTI backups. Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. See IRS Publication 1075 Section 9.3.6.5 (page 66) for further guidance.

Agency SSR Response:

9.3.6.6 CP-7: Alternate Processing Site

Describe how the agency identifies alternate processing sites that provide information security safeguards to meet the minimum protection standards and the disclosure provisions of IRC 6103.

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

The agency must identify alternate processing sites and/or telecommunications capabilities, and initiate necessary agreements to facilitate secure resumption of information systems used to process, store and transmit FTI if the primary processing site and/or primary telecommunications capabilities become unavailable. See IRS Publication 1075 Section 9.3.6.6 (pages 66-67) for further guidance.

Agency SSR Response:

9.3.6.7 CP-9: Information System Backup

Describe 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. Include how the agency protects the confidentiality of backup information at storage locations pursuant to IRC 6103 requirements.

System-level information includes but not limited to, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. See IRS Publication 1075 Section 9.3.6.7 (page 67) for further guidance.

Agency SSR 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.

Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures. See IRS Publication 1075 Section 9.3.6.8 (page 67) for further guidance.

Agency SSR 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
   - Include details regarding policy review/update (every three years or if there is a significant change)

B) Identification and authentication procedures to facilitate the policy and IA related security controls
   - Include details regarding policy review/update (annually)

The agency must develop and maintain identification and authentication policies and procedures. See IRS Publication 1075 Section 9.3.7.1 (page 67) for further guidance.

Agency SSR Response:

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

Describe how the agency's information system(s) must be configured to uniquely identify organizational/agency users (or processes acting on behalf of agency users).

A) Document if, and describe 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)

B) Document if, and describe 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. *Note*: NIST SP 800-63 allows the use of software tokens (CE11)

The information system must be configured to uniquely identify users, devices, and processes via the assignment of unique user accounts and validate users (or processes acting on behalf of users) using standard authentication methods such as passwords, tokens, smart cards, or biometrics. See IRS Publication 1075 Section 9.3.7.2 (pages 67-68) for further guidance.

Agency SSR Response:

9.3.7.3 IA-3: Device Identification and Authentication

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

Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. See IRS Publication 1075 Section 9.3.7.3 (page 68) for further guidance.

Agency SSR 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; and assigns the identifier to the intended individual, group, role, or device

C) Describe how the agency prevents reuse of identifiers

D) Describe if, and how the agency disables information system identifiers after a period of user inactivity

Publication 1075 requirement: Disable the identifier after 120 days

See IRS Publication 1075 Section 9.3.7.4 (page 68) for further guidance.

Agency SSR Response:

9.3.7.5 IA-5: Authenticator Management

Describe how the agency manages information system authenticators (or passwords).

A) Describe how the agency implements the following authenticator requirements:

- Verifies, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator
- Establishes initial authenticator content for authenticators defined by the agency and ensures authenticators have sufficient strength of mechanism for their intended use
- Establishes and implements administrative procedure(s) for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators
- Changes default content of authenticators prior to information system installation
- Establishes minimum and maximum lifetime restrictions and reuse conditions for authenticators
- Changes/refreshes authenticators on a regular basis (include frequency in agency response)
- Protects authenticator content from unauthorized disclosure and modification; and requires individuals to take, and having devices implement, specific security safeguards to protect authenticators
- Changes authenticators for group/role accounts when membership to those accounts changes

B) 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
- Enforces password minimum lifetime restriction of one day
- Enforces non-privileged account passwords to be changed at least every 90 days; and enforces privileged account passwords to be changed at least every 60 days
- Prohibits password reuse for 24 generations
- Allows the use of a temporary password for system logons requiring an immediate change to a permanent password
- Password-protects system initialization (boot) settings
- Stores and transmits only encrypted representations of passwords

See IRS Publication 1075 Section 9.3.7.5 (pages 68-69) for further guidance.

Agency SSR 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.

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. See IRS Publication 1075 Section 9.3.7.6 (page 69) for further guidance.

Agency SSR 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.

Publication 1075 requirement: 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/.

The agency shall work to ensure these modules are compliant with NIST guidance, including FIPS 140-2 compliance whenever agencies are employing cryptographic modules. See IRS Publication 1075 Section 9.3.7.7 (page 69) for further guidance.

Agency SSR 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).

Non-organizational users include information system users other than organizational users explicitly covered by IA-2. See IRS Publication 1075 Section 9.3.7.8 (page 69) for further guidance.

Agency SSR 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
   - Include details regarding policy review/update (every three years or if there is a significant change)

B) Incident response procedures to facilitate the policy and IR related security controls
   - Include details regarding policy review/update (annually)

The agency must develop and maintain incident response policies and procedures. See IRS Publication 1075 Section 9.3.8.1 (page 70) for further guidance.

Agency SSR 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.

A) Document if, and how the agency provides incident response training to information system users consistent with assigned roles and responsibilities

B) Describe when training occurs and at what frequency

Publication 1075 requirement: Incident response training shall occur prior to assuming an incident response role or responsibility, when required by information system changes, and annually thereafter

The agency must train personnel in their incident response roles on the information system and FTI. Incident response training must provide individuals with an understanding of incident handling capabilities for security events, including preparation, detection and analysis, containment, eradication, and recovery. See IRS Publication 1075 Section 9.3.8.2 (page 70) for further guidance.

Agency SSR Response:

9.3.8.3 IR-3: Incident Response Testing

Describe how the agency entrusted with FTI tests and/or exercises the incident response capability for the information system.

A) Describe how the agency performs tabletop exercises using scenarios that include a breach of FTI

Publication 1075 requirement: All employees and contractors with significant FTI incident response capabilities, including technical personnel responsible for maintaining consolidated data centers and off-site storage, must be included in tabletop exercises

B) 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.

The agency shall test and/or exercise the incident response capability for the information system at least annually to determine the incident response effectiveness and document the results. Incident response testing includes: use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. See IRS Publication 1075 Section 9.3.8.3 (page 70) for further guidance.

Agency SSR Response:

9.3.8.4 IR-4: Incident Handling

Describe how the agency implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

A) Describe how the agency coordinates incident handling activities with contingency planning activities; and incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implement the resulting changes accordingly

The agency must routinely track and document information system security incidents potentially affecting the confidentiality of FTI. See IRS Publication 1075 Section 9.3.8.4 (page 71) for further guidance.

Agency SSR 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.

The agency must promptly report security incident information to the appropriate Agent-in-Charge, (TIGTA), and any time there is a compromise to FTI. See IRS Publication 1075 Section 9.3.8.5 (page 71) for further guidance.

Agency SSR Response:

9.3.8.6 IR-6: Incident Reporting

Describe the agency's policy to immediately report incident information any time there is a compromise to FTI to the appropriate Agent-in-Charge, TIGTA, and the IRS following the requirements of Publication 1075, Section 10: *Reporting Improper Inspections or Disclosures*.

Publication 1075 requirement: Require personnel to report suspected security incidents to internal agency incident response resources upon discovery of the incident; and contact 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

The agency shall also provide an security incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the agency's incident response capability. Incidents involving FTI are required to be reported to TIGTA and to IRS within 24 hours of discovery of the incident. See IRS Publication 1075 Section 9.3.8.6 (page 71) for further guidance.

Agency SSR 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.

Incident response support resources provided by organizations include: help desks, assistance groups, and access to forensics services, when required. See IRS Publication 1075 Section 9.3.8.7 (page 71) for further guidance.

Agency SSR Response:

9.3.8.8 IR-8: Incident Response Plan

Describe how the agency develops and maintains an Incident Response Plan (IRP) that provides the agency with a roadmap for implementing its incident response capability.

A) Describe how the agency addresses the following in the IRP :

- Describes the structure of the incident response capability and 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 and 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
- Ensures the document is reviewed and approved by designated agency officials

B) Describe how the IRP is distributed to authorized incident response personnel and protected from unauthorized disclosure and modification

C) Describe how the IRP is reviewed, updated, and communicated on a regular basis

Publication 1075 requirement: Review the incident response plan at a minimum on an annual basis or as an after-action review

See IRS Publication 1075 Section 9.3.8.8 (pages 71-72) for further guidance.

Agency SSR 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

Information spillage refers to instances where either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required. See IRS Publication 1075 Section 9.3.8.9 (page 72) for further guidance.

Agency SSR 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:

C) A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
- Include details regarding policy review/update (every three years or if there is a significant change)

D) System maintenance procedures to facilitate the policy and MA related security controls
- Include details regarding policy review/update (annually)

The agency shall develop and maintain system maintenance policies and procedures. See IRS Publication 1075 Section 9.3.9.1 (pages 72-73) for further guidance.

Agency SSR 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 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

Publication 1075 requirement: The designated agency officials shall explicitly approve the removal of the information system or system components from agency facilities for off-site maintenance or repairs

C) 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

D) 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

The agency must ensure that maintenance is scheduled, performed, and documented. The control applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity. System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. See IRS Publication 1075 Section 9.3.9.2 (page 73) for further guidance.

Agency SSR Response:

9.3.9.3 MA-3: Maintenance Tools

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

The agency must approve, control, and routinely monitor the use of information system maintenance tools. Maintenance tools include hardware, software, and firmware. See IRS Publication 1075 Section 9.3.9.3 (page 73) for further guidance.

Agency SSR Response:

9.3.9.4 MA-4: Non-Local Maintenance

Describe how the agency approves, controls, and monitors non-local maintenance and diagnostic activities. Include how the agency:

- 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
- Employs multi-factor authenticator in the establishment of non-local maintenance and diagnostic sessions
- Maintains records for non-local maintenance and diagnostic activities
- Terminates session and network connections when non-local maintenance is completed
- Documents policies and procedures for the establishment and use of non-local maintenance and diagnostic connections (CE2)

The agency must approve, control, and routinely monitor the use of remotely-executed maintenance and diagnostic activities. Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. See IRS Publication 1075 Section 9.3.9.4 (page 73) for further guidance.

Agency SSR 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:

- Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel
- Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations
- 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

The agency shall ensure that it allows only authorized personnel to perform maintenance on the information system. See IRS Publication 1075 Section 9.3.9.5 (page 74) for further guidance.

Agency SSR 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
- Include details regarding policy review/update (every three years or if there is a significant change)

B) Media protection procedures to facilitate the policy and MP related security controls
- Include details regarding policy review/update (annually)

Note: *Information system media is defined to include both digital and non-digital media.*

The agency must develop and maintain media access policies and procedures. See IRS Publication 1075 Section 9.3.10.1 (page 74) for further guidance.

Agency SSR 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.

The agency shall restrict access to information system media to authorized individuals, where this media contains FTI. See IRS Publication 1075 Section 9.3.10.2 (page 74) for further guidance.

Agency SSR 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.

Publication 1075 requirement: 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.

The agency should physically control and securely store information system media within controlled areas, where this media contains FTI. See IRS Publication 1075 Section 9.3.10.3 (page 74) for further guidance.

Agency SSR Response:

9.3.10.4 MP-4: Media Storage

Describe how the agency physically controls and securely stores information system media containing FTI.

A) Document details how the agency 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.

See IRS Publication 1075 Section 9.3.10.4 (page 75) for further guidance.

Agency SSR Response:

9.3.10.5 MP-5: Media Transport

Describe how the agency protects and controls digital (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs) and non-digital (e.g., paper) media during transport outside of controlled areas.

A) Describe how the agency addresses:
- Maintains accountability for information system media during transport outside of controlled areas
- 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)
- Restricts the activities associated with the transport of information system media to authorized personnel

B) 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.

All media being transported from the IRS must employ the use of encryption. See IRS Publication 1075 Section 9.3.10.5 (page 75) for further guidance.

Agency SSR Response:

9.3.10.6 MP-6: Media Sanitization

Describe how the agency 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.

A) Describe how the agency employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information

B) Describe how the agency 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.

The agency shall sanitize information system media prior to disposal or release for reuse. See IRS Publication 1075 Section 9.3.10.6 (pages 75-76) for further guidance.

Agency SSR 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.

Physical and Environmental Protection (PE) controls are applicable to the data center where systems reside, as well as any office location where employees access FTI. For each applicable location, we will be looking for specific location controls.

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
- Include details regarding policy review/update (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
- Include details regarding policy review/update (annually)

The agency must develop and maintain physical and environmental protection policies and procedures. See IRS Publication 1075 Section 9.3.11.1 (page 76) for further guidance

Agency SSR 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.

A) Describe how the agency develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides

B) Describe how the agency issues authorization credentials for facility access

C) Describe how the agency reviews the access list detailing authorized facility access by individuals
Publication 1075 requirement: At least annually

D) Describe how the agency removes individuals from the facility access list when access is no longer required

E) Describe how the agency 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.*

Below are examples of delineation of location based controls:
1) Data Center
2) Field Office location
3) Off-site Storage location

See IRS Publication 1075 Section 9.3.11.2 (pages 76-77) for further guidance.

Agency SSR Response:

9.3.11.3 PE-3: Physical Access Control

Describe how the agency enforces physical access authorizations at entry/exit points to facilities where the information systems that receive, process, store, or transmit FTI reside by. Include how the agency addresses:

- Verifies individual access authorizations before granting access to the facility
- Controls ingress/egress to the facility using physical access control systems/devices or guards
- Maintains physical access audit logs for entry/exit points
- Provides security safeguards to control access to areas within the facility officially designated as publicly accessible
- Escorts visitors and monitor visitor activity
- Secures keys, combinations, and other physical access devices
- Maintains an inventory of physical access devices
- 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.*

Barriers include: secured perimeter, security room, badge access, and security container.
A locked server rack can serve as the second barrier, as long as someone with authorized access to FTI maintains control of the key within a multi-tenant data center environment. See IRS Publication 1075 Section 9.3.11.3 (page 77) for further guidance.

Agency SSR 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.

Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. See IRS Publication 1075 Section 9.3.11.4 (page 77) for further guidance.

Agency SSR 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.

See IRS Publication 1075 Section 9.3.11.5 (page 77) for further guidance.

Agency SSR Response:

9.3.11.6 PE-6: Monitoring Physical Access

Describe how the agency monitors physical access to the facility where the information system resides to detect and respond to physical security incidents. Include how the agency:

- Reviews physical access logs annually
- Coordinates results of reviews and investigations with the agency incident response capability
- 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 security incident response capabilities include but not limited to investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. See IRS Publication 1075 Section 9.3.11.6 (pages 77-78) for further guidance.

Agency SSR Response:

9.3.11.7 PE-8: Visitor Access Records

Describe how the agency maintains visitor access records to the facility where the information system resides. Document the frequency in which visitor access records are reviewed.

Publication 1075 requirement: 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.*

Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas. See IRS Publication 1075 Section 9.3.11.7 (page 78) for further guidance.

Agency SSR 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.

See IRS Publication 1075 Section 9.3.11.8 (page 78) for further guidance.

Agency SSR Response:

9.3.11.9 PE-17: Alternate Work Site

Describe how the agency employs IRS Office of Safeguards requirements at alternate work sites. Include how the agency:

- Assesses, as feasible, the effectiveness of security controls at alternate work sites
- 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.*

Alternate work sites may include: agency facilities, field offices, or private residences of employees.
See IRS Publication 1075 Section 9.3.11.9 (page 78) for further guidance.

Agency SSR 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.

Physical and environmental hazards include: flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. Please also document how user workstations (permitted to view/access FTI) are positioned to minimize the risk of shoulder surfing. See IRS Publication 1075 Section 9.3.11.10 (page 78) for further guidance.

Agency SSR 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
   - Include details regarding policy review/update (every three years or if there is a significant change)

B) Security planning procedures to facilitate the policy and PL related security controls
   - Include details regarding policy review/update (annually)

The agency must develop and maintain security planning policies and procedures. See IRS Publication 1075 Section 9.3.12.1 (page 79) for further guidance.

Agency SSR Response:

9.3.12.2 PL-2: System Security Plan

Describe how the agency develops and approves an accurate Safeguards Security Report. The agency SSR satisfies this requirement (Section 7.0, *Reporting Requirements—6103(p)(4)(E)*, of Publication 1075).

A) Describe how the agency:

- Develops an SSR that is consistent with the agency's safeguarding requirements, and explicitly defines the information systems that receive, process, store, or transmit FTI
- Describes the how the SSR defines the operational context of the information system in terms of missions and business processes, and 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 and identifies 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
- Ensures the SSR is reviewed and approved by the authorizing official or designated representative prior to plan implementation

B) Describe how the agency distributes copies of the SSR and communicates subsequent changes to designated agency officials and the IRS Office of Safeguards; and protects the SSR from unauthorized disclosure and modification

The agency must develop and maintain a system security plan by describing the security requirements, current controls and planned controls for protecting agency information systems and FTI. If the agency does not have System Security Plans (SSP) for IT systems containing FTI, please reference the agency's Safeguard Security Report (SSR) as evidence for this security control. See IRS Publication 1075 Section 9.3.12.2 (pages 79-80) for further guidance.

Agency SSR Response:

9.3.12.3 PL-4: Rules of Behavior

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

A) Describe how the agency 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

Publication 1075 requirement: Receive a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system

B) Describe how the agency reviews and updates the rules of behavior, and document how the agency 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

C) Document if, and how the agency 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

The agency must develop and maintain a set of rules describing their responsibilities and expected behavior for information system use for users of the information system.

The Rules of Behavior is different than annual disclosure awareness training. This is generally an agency document that is created for all users to accept computer use guidelines and behavior.

See IRS Publication 1075 Section 9.3.12.3 (page 80) for further guidance.

Agency SSR 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
- Include details regarding policy review/update (every three years or if there is a significant change)

B) Personnel security procedures to facilitate the policy and PS related security controls
- Include details regarding policy review/update (annually)

The agency shall develop and maintain personnel security policies and procedures. See IRS Publication 1075 Section 9.3.13.1 (page 80) for further guidance.

Agency SSR Response:

9.3.13.2 PS-2: Position Risk Designation

Describe how the agency assigns a risk designation to all agency positions, establishes screening criteria for individuals filling those positions, and reviews and updates position risk designations.

Publication 1075 requirement: Review and update position risk designations annually

The agency shall assign risk designations to all positions and establish screening criteria for individuals filling those positions. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances). See IRS Publication 1075 Section 9.3.13.2 (page 80) for further guidance.

Agency SSR Response:

9.3.13.3 PS-3: Personnel Screening

Describe how the agency screens individuals prior to authorizing access to the information system, and rescreens individuals according to agency-defined conditions requiring rescreening.

The agency shall ensure that individuals are screened before authorizing access to information systems and information. Agencies may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems. See IRS Publication 1075 Section 9.3.13.3 (page 81) for further guidance.

Agency SSR Response:

9.3.13.4 PS-4: Personnel Termination

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

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

The agency shall terminate information system access, conduct exit interviews, and ensure return of all information system-related property when employment is terminated. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Timely execution of termination actions is essential for individuals terminated for cause. See IRS Publication 1075 Section 9.3.13.4 (page 81) for further guidance.

Agency SSR Response:

9.3.13.5 PS-5: Personnel Transfer

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

- 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
- Initiates transfer or reassignment actions following the formal transfer action
- Modifies access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer
- Notifies designated agency personnel, as required

This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Actions that may be required for personnel transfers or reassignments to other positions within agencies include: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts. See IRS Publication 1075 Section 9.3.13.5 (page 81) for further guidance.

Agency SSR 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:

- Develops and documents access agreements for agency information systems
- Reviews and updates the access agreements, at least annually

A) Describe how the agency ensures that individuals requiring access to agency information and information systems:

- Sign appropriate access agreements prior to being granted access
- Re-sign access agreements to maintain access to agency information systems when access agreements have been updated or at least annually

The agency shall ensure that appropriate access agreements are completed before authorizing access to users requiring access to the information system and FTI. Access agreements include: nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. See IRS Publication 1075 Section 9.3.13.6 (page 81) for further guidance.

Agency SSR Response:

9.3.13.7 PS-7: Third-Party Personnel Security

Describe how the agency establishes personnel security requirements, including security roles and responsibilities for third-party providers. Include how the agency:

- Requires third-party providers to comply with personnel security policies and procedures established by the agency
- Documents personnel security requirements
- 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
- Monitors provider compliance

The agency shall ensure that personnel security requirements are established for third-party providers and monitored for provider compliance. See IRS Publication 1075 Section 9.3.13.7 (page 82) for further guidance.

Agency SSR Response:

9.3.13.8 PS-8: Personnel Sanctions

Describe how the agency employs a formal sanctions process for individuals failing to comply with established information security policies and procedures. Document how the agency notifies designated agency personnel when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

The agency shall ensure that formal sanctions process for personnel, who fail to comply with established information security policies, as this relates to FTI, is established. See IRS Publication 1075 Section 9.3.13.8 (page 82) for further guidance.

Agency SSR 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
   - Include details regarding policy review/update (every three years or if there is a significant change)

B) Risk assessment procedures to facilitate the policy and RA related security controls
   - Include details regarding policy review/update (annually)

The agency must have in place, risk assessment policy and procedures that are disseminated to the appropriate parties and updated on a regular basis. This includes, but is not limited to, risk assessments and risk assessment updates.
See IRS Publication 1075 Section 9.3.14.1 (page 82) for further guidance.

Agency SSR Response:

9.3.14.2 RA-3: Risk Assessment

Describe how the agency 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. Include how the agency:

- Documents risk assessment results in a risk assessment report
- Reviews risk assessment results at least annually
- Disseminates risk assessment results to designated agency officials
- 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

The agency must conduct a security assessment that is in accordance with Federal Information Processing Standards (FIPS) publication 199 that will determine the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency regarding the use of FTI. See IRS Publication 1075 Section 9.3.14.2 (page 83) for further guidance.

Agency SSR Response:

9.3.14.3 RA-5: Vulnerability Scanning

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

A) Define the frequency at which vulnerability scans are conducted

Publication 1075 requirement: At a minimum monthly for all systems and when new vulnerabilities potentially affecting the system/applications are identified and reported

B) Describe how the agency 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) Describe how the agency analyzes vulnerability scan reports and results from security control assessments, and remediates legitimate vulnerabilities in accordance with an assessment of risk

D) Describe how the agency 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)

E) Describe if, and how the agency employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned (CE1)

The agency must specify the frequency that scans are performed on systems containing FTI to identify potential vulnerabilities in the system. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. If penetration tests are conducted against the agency, please state so in the agency's response to RA-5: Vulnerability Scanning. See IRS Publication 1075 Section 9.3.14.3 (page 83) for further guidance.

Agency SSR 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

- Include details regarding policy review/update (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

- Include details regarding policy review/update (annually)

The agency must develop and maintain necessary system and services acquisition policies and procedures. See IRS Publication 1075 Section 9.3.15.1 (page 84) for further guidance.

Agency SSR Response:

9.3.15.2 SA-2: Allocation of Resources

Describe how the agency determines information security requirements for the information system or information system service in mission/business process planning. Include how the agency:

- 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
- Establishes a discrete line item for information security in agency programming and budgeting documentation

The agency must document and allocate as part of its capital planning and investment control process, the resources required to adequately protect the information system. See IRS Publication 1075 Section 9.3.15.2 (page 84) for further guidance.

Agency SSR Response:

9.3.15.3 SA-3: System Development Life Cycle

Describe how the agency manages the information system using an SDLC that incorporates information security considerations. Include how the agency:

- Defines and documents information security roles and responsibilities throughout the SDLC
- Identifies individuals having information security roles and responsibilities
- Integrates the agency information security risk management process into SDLC activities

The agency must manage the information system using a system development life cycle methodology that includes information security considerations whenever information systems contain FTI. A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of agency information systems. See IRS Publication 1075 Section 9.3.15.3 (page 84) for further guidance.

Agency SSR Response:

9.3.15.4 SA-4: Acquisition Process

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

A) 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)

NOTE: The agency must include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk whenever information systems contain FTI. See IRS Publication 1075 Section 9.3.15.4 (pages 84-85) for further guidance.

Agency SSR Response:

9.3.15.5 SA-5: Information System Documentation

Describe how the agency develops and maintains information system documentation.

A) Describe how the agency 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) Describe how the agency 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) Describe how the agency documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent

D) Describe how the agency stores and protects documentation, as required; and distributes documentation to designated agency officials

The agency must obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system whenever information systems contain FTI. See IRS Publication 1075 Section 9.3.15.5 (page 85) for further guidance.

Agency SSR 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.

Security engineering principles include: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. See IRS Publication 1075 Section 9.3.15.6 (page 86) for further guidance.

Agency SSR Response:

9.3.15.7 SA-9: External Information System Services

Describe how the agency 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. Include how the agency:

- Defines and documents government oversight and user roles and responsibilities with regard to external information system services
- Monitors security control compliance by external service providers on an ongoing basis
- 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).*

See IRS Publication 1075 Section 9.3.15.7 (page 86) for further guidance.

Agency SSR 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:

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

See IRS Publication 1075 Section 9.3.15.8 (page 86) for further guidance.

Agency SSR 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:

- Create and implement a security assessment plan
- Perform security testing/evaluation
- Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation
- Implement a verifiable flaw remediation process
- Correct flaws identified during security testing/evaluation

The information system developers shall create a security test and evaluation plan, implement the plan, and document the results. Developmental security testing/evaluation occur at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. See IRS Publication 1075 Section 9.3.15.9 (page 87) for further guidance.

Agency SSR 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.

Support for information system components includes, but not limited to, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components (e.g., when vendors are no longer providing critical software patches), provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components.

Failure to implement this security control can lead to a catastrophic (or soon to be, critical) finding that warrants remediation. In your response, please document if any technologies receiving, storing, processing and/or transmitting FTI deployed in the environment are no longer supported.

See IRS Publication 1075 Section 9.3.15.10 (page 87) for further guidance.

Agency SSR 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
- Include details regarding policy review/update (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
- Include details regarding policy review/update (annually)

The agency must develop and maintain system and communications policies and procedures. See IRS Publication 1075 Section 9.3.16.1 (page 87) for further guidance.

Agency SSR 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.

Information system management functionality includes: functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes; web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls. See IRS Publication 1075 Section 9.3.16.2 (page 87) for further guidance.

Agency SSR 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.

This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. See IRS Publication 1075 Section 9.3.16.3 (page 87) for further guidance.

Agency SSR 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.*

A variety of technologies exist to limit, or in some cases, eliminate, the effects of denial of service attacks. Boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks. See IRS Publication 1075 Section 9.3.16.4 (page 88) for further guidance.

Agency SSR Response:

9.3.16.5 SC-7: Boundary Protection

Describe how the agency protects the network boundary hosting FTI.

A) Describe how the agency monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. Include how the agency:
   - Implements sub-networks for publicly accessible system components that are physically and logically separated from internal agency networks
   - Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with agency security architecture requirements

B) Describe how the agency limits the number of external network connections to the information system (CE3)

C) Describe 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; and 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)

D) 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)

E) 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.*

The information system shall be configured to monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. See IRS Publication 1075 Section 9.3.16.5 (pages 88-89) for further guidance.

Managed interfaces include: gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within the security architecture (e.g., routers protecting firewalls or application gateways residing on protected sub networks).

Agency SSR 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.

A) Describe how the agency protects the confidentiality and integrity of transmitted information

B) Describe how the agency 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).

The information system must protect the confidentiality and integrity of FTI during electronic transmission. See IRS Publication 1075 Section 9.3.16.6 (page 89) for further guidance.

Agency SSR 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 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.*

This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. See IRS Publication 1075 Section 9.3.16.7 (page 89) for further guidance.

Agency SSR 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.*

When Public Key Infrastructure (PKI) is used, the agency shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures. Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Agencies should manage trust stores to ensure that only approved trust anchors are in such trust stores. See IRS Publication 1075 Section 9.3.16.8 (page 89) for further guidance.

Agency SSR 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.

When cryptography (encryption) is employed within the information system, the system must perform all cryptographic operations using Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules with approved modes of operation. See IRS Publication 1075 Section 9.3.16.9 (page 90) for further guidance.

Agency SSR Response:

9.3.16.10 SC-15: Collaborative Computing Devices

Describe how the agency prohibits remote activation of collaborative computing devices and provide 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.*

The information system shall prohibit remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users. See IRS Publication 1075 Section 9.3.16.10 (page 90) for further guidance.

Agency SSR 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.

The agency shall establish PKI policies and practices, as necessary. For all certificates, agencies should manage information system trust stores to ensure only approved trust anchors are in the trust stores. See IRS Publication 1075 Section 9.3.16.11 (page 90) for further guidance.

Agency SSR 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:

- Defines acceptable and unacceptable mobile code and mobile code technologies
- Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies
- 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).*

The agency shall establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously. See IRS Publication 1075 Section 9.3.16.12 (page 90) for further guidance.

Agency SSR Response:

9.3.16.13 SC-19: Voice over Internet Protocol

Describe how the agency establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously. Document how the agency 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.*

The agency shall establish, document and control usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies. See IRS Publication 1075 Section 9.3.16.13 (pages 90-91) for further guidance.

Agency SSR 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.*

The information system shall provide mechanisms to protect the authenticity of communications sessions. Authenticity protection includes: protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions. See IRS Publication 1075 Section 9.3.16.14 (page 91) for further guidance.

Agency SSR 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: 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. The confidentiality and integrity of information at rest shall be protected when located on a secondary (non-mobile) storage device (e.g., disk drive, tape drive) with cryptography mechanisms. See IRS Publication 1075 Section 9.3.16.15 (page 91) for further guidance.

Agency SSR 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:

D) A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
- Include details regarding policy review/update (every three years or if there is a significant change)

E) System and information integrity procedures to facilitate the policy and SI related security controls
- Include details regarding policy review/update (annually)

The agency must develop and maintain system and information integrity policies and procedures. See IRS Publication 1075 Section 9.3.17.1 (pages 91-92) for further guidance.

Agency SSR 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.

A) Describe how the agency identifies, reports, and corrects information system flaws
B) Describe how the agency tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation
C) Describe how the agency installs security-relevant software and firmware updates based on severity and associated risk to the confidentiality of FTI
D) Describe how the agency incorporate flaw remediation into the agency configuration management process
E) Document if, and how the agency centrally manage the flaw remediation process (CE1)

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

The agency must identify, report, and correct information system flaws. See IRS Publication 1075 Section 9.3.17.2 (page 92) for further guidance.

Agency SSR Response:

9.3.17.3 SI-3: Malicious Code Protection

Describe how the agency applies malicious code protection mechanisms.

A) Describe how the agency employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code
B) Describe how the agency updates malicious code protection mechanisms whenever new releases are available in accordance with agency configuration management policy and procedures
C) Describe how the agency configures malicious code protection mechanisms

Publication 1075 requirement: 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; and address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system

D) Document if the agency centrally manages malicious code protection mechanisms (CE1)
E) Document if the agency automatically updates malicious code protection mechanisms (CE2)

The information system must implement protection against malicious code (e.g., viruses, worms, Trojan horses) that, to the extent possible, includes a capability for automatic updates.

Information system entry and exit points include: firewalls, electronic mail servers, Web servers, proxy servers, remote access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g. UUENCODE, Unicode), contained within compressed or hidden files or hidden in files using steganography. Malicious code can be transported by different means, including: Web accesses, electronic mail, electronic mail attachments, and portable storage devices.

See IRS Publication 1075 Section 9.3.17.3 (pages 92-93) for further guidance.

Agency SSR Response:

9.3.17.4 SI-4: Information System Monitoring

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

A) Describe how the agency monitors the information system to detect: attacks and indicators of potential attacks; and unauthorized local, network, and remote connections

B) Describe how the agency identifies unauthorized use of the information system

C) Describe how the agency 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) Describe how the agency protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion

E) Describe how the agency 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) Describe how the agency provides information system monitoring information to designated agency officials (as needed)

G) Describe how the agency 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) Document if the agency employs automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications (CE11)

I) Document if the agency implements host-based monitoring mechanisms (e.g., Host intrusion prevention system (HIPS)) on information systems that receive, process, store, or transmit FTI (CE23)

J) Describe how the agency monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions (CE4)

K) Describe how the agency alerts designated agency officials when indications of compromise or potential compromise occur (CE5)

L) Describe how the agency notifies designated agency officials of detected suspicious events and take necessary actions to address suspicious events (CE7)

Intrusion detection tools and techniques must be employed to monitor system events, detect attacks, and identify unauthorized use of the information system and FTI. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). See IRS Publication 1075 Section 9.3.17.4 (pages 93-94) for further guidance.

Agency SSR Response:

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

Describe how the agency receives and responds to security alerts, advisories, and directives.

A) Describe if, and how the agency receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis

B) Describe how the agency generates internal security alerts, advisories, and directives as deemed necessary

C) Describe how the agency disseminates security alerts, advisories, and directives to designated agency officials; and implements security directives in accordance with established time frames or notify the issuing agency of the degree of noncompliance

The agency shall receive and review information system security alerts/advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response. See IRS Publication 1075 Section 9.3.17.5 (pages 94-95) for further guidance.

Agency SSR Response:

9.3.17.6 SI-8: Spam Protection

Describe how the employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages, and document the frequency in which the agency updates spam protection mechanisms.

Publication 1075 requirement: Update spam protection mechanisms when new releases are available in accordance with agency configuration management policy and procedures

Information system entry and exit points include firewalls, electronic mail servers, Web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including electronic mail, electronic mail attachments, and Web accesses. Spam protection mechanisms include, signature definitions. See IRS Publication 1075 Section 9.3.17.6 (page 95) for further guidance.

Agency SSR Response:

9.3.17.7 SI-10: Information Input Validation

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

Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks. See IRS Publication 1075 Section 9.3.17.7 (page 95) for further guidance.

Agency SSR Response:

9.3.17.8 SI-11: Error Handling

Describe how the agency generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. Document if, and how error messages are only to designated agency officials.

Agencies should carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. See IRS Publication 1075 Section 9.3.17.8 (page 95) for further guidance.

Agency SSR 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.

The agency must handle and retain output from the information system, as necessary to document that specific actions have been taken. See IRS Publication 1075 Section 9.3.17.9 (page 95) for further guidance.

Agency SSR 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.*

See IRS Publication 1075 Section 9.3.17.10 (page 95) for further guidance.

Agency SSR 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.*

Please include reference to a policy and/or procedure that addresses appropriate security roles and responsibilities. Additionally, please include the name and contact information for the appointed Senior Information Security Officer and a list of his/her responsibilities. See IRS Publication 1075 Section 9.3.18.1 (page 96) for further guidance.

Agency SSR 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:

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.

If the agency does not employ a cloud computing environment, this control will be Not Applicable. If the agency does (and FTI is received, processed, stored, or transmitted throughout the cloud), please ensure responses above are documented in this section. See IRS Publication 1075 Section 9.4.1 (pages 97-98) for further guidance.

Agency SSR 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? Data Warehouse controls are only applicable if the Data Warehouse is implemented in computer system(s) that store, transmit, or process FTI. If applicable, please ensure all data warehouse controls are documented and included in the agency's responses throughout Section 9. If a Data Warehouse environment is not applicable to your agency's use of child support information, containing FTI, please mark each Data Warehouse section as Not Applicable.	☐ 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; and

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.

Please ensure responses for above are documented in this section. If FTI is prohibited from inclusion within emails or email attachments, please describe how the agency documents and distributes such a policy. See IRS Publication 1075 Section 9.4.3 (pages 98-99) for further guidance.

Agency SSR 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; and
D) Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes:
   a. A notification of the sensitivity of the data and the need for protection; and
   b. A notice to unintended recipients to telephone the sender—collect, if necessary—to report the disclosure and confirm destruction of the information.

See IRS Publication 1075 Section 9.4.4 (page 99) for further guidance. If FTI is prohibited from inclusion within fax communications, please describe how the agency documents and distributes such a policy.

Agency SSR 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; and
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.

See IRS Publication 1075 Section 9.4.5 (pages 99-100) for further guidance.

Agency SSR 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? If yes, agencies wishing to use live FTI data in pre-production must submit a request to the DCSS ISO mailbox: info.security@dcss.ca.gov for authority to use live data for testing. The request should provide a detailed explanation of the safeguards in place to protect the data and the necessity for using live data during testing. See IRS Publication 1075 Section 9.4.5 (pages 99-100) for further guidance.	☐ 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; and
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).

See IRS Publication 1075 Section 9.4.9 (page 103) for further guidance. If FTI is prohibited from such devices, please describe how the agency documents and distributes such a policy.

Agency SSR 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) Fiber 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.

See IRS Publication 1075 Section 9.4.11 (pages 104-105) for further guidance. If FTI is prohibited from such devices, please describe how the agency documents and distributes such a policy.

Agency SSR 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? These are specific IRS requirements for FTI that is processed in virtual environments. Focus on the technical requirements as the notification requirements will only be applicable after the systems go live.	☐ 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.

These are specific IRS requirements for VoIP networks that process FTI. See IRS Publication 1075 Section 9.4.15 (pages 107-108) for further guidance.

Agency SSR 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; and
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.

See IRS Publication 1075 Section 9.4.16 (page 108) for further guidance.

Agency SSR 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.

See IRS Publication 1075 Section 9.4.17 (pages 108-109) for further guidance.

Agency SSR 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.

See IRS Publication 1075 Section 9.4.18 (pages 109-110) for further guidance.

Agency SSR Response:

SAFEGUARDS SECURITY REPORT (SSR), FORMERLY CALLED SAFEGUARDS ACTIVITY REPORT (SAR) - TRAINING SLIDE

OBJECTIVE

- Pursuant to Internal Revenue Code (IRC) Section 6103, recipient agencies that legally receive federal tax information (FTI) directly from either the IRS or from secondary sources (e.g. Social Security Administration, Office of Child Support Enforcement), 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.*

- The Safeguards Security Report (SSR), formerly called the Safeguards Activity Report (SAR) is a new Internal Revenue Service (IRS) requirement that reports how FTI is processed and safeguarded from unauthorized disclosure by recipient local child support agencies (LCSAs).

A SSR is a certification that:

- 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.
- Addresses all Outstanding Actions identified from the prior year's SSR submittals.
- Assist the DCSS Information Security Office (DCSS ISO) in the joint effort of protecting the confidentiality of FTI.
- Report all data incidents involving FTI to the DCSS ISO at info.security@dcss.ca.gov mailbox timely and cooperate with the investigations.
- Support the on-site Safeguard review conducted by DCSS ISO or the IRS to assess agency compliance.
- Support timely mitigation of identified risk to FTI in the agency's Corrective Action Plan (CAP)

INSTRUCTIONS TO COMPLETE

- Option 1, 2 and 3 LCSA staff responsible for agency safeguard activities needs to complete SSR Sections 1 through 8 that address:
- Agency Information - Director Name, title, address, etc.
- Current Period Safeguard Activities - activities conducted during the reporting period.
- Changes to Safeguarding Procedures – safeguard changes made during the reporting period.
- Safeguarding Procedures - procedures established and used for ensuring the confidentiality of FTI that is received, processed, stored, or transmitted.
- FTI Flow and Processing - description of the FTI the agency receives and whether the data is received through electronic or non-electronic methods.
- System of Records - description of permanent record(s) (logs) used to document requests for, receipt of, distribution of, and disposition of the FTI.
- Disposal - A description of the method(s) of FTI disposal.

INSTRUCTIONS – Cont.

- The Option 2 and 3 LCSAs must also complete SSR Section 9, Information Security Controls. The questions in Section 9 are required for all agencies that receive FTI and describe the agency policies, procedures and the security controls in place to protect child support information, containing FTI that is downloaded, stored, extracted, printed, etc. from DCSS systems.
- We encourage Option 2 and 3 LCSAs to work with county IT representatives to complete Section 9.

NOTE:

Option 1 LCSAs are exempt from completing Section 9.

SUBMITTAL INSTRUCTIONS

- The SSR reporting period is February 1 through January 31.
- LCSAs must update and securely submit an SSR to the DCSS Information Security Office mailbox by January 31, 2015, and annually thereafter.
- Do not submit the completed SSR to the IRS.
- The DCSS Information Security Office will incorporate responses into one SSR document for submittal to the IRS.

QUESTIONS

If you have any questions or concerns regarding this information, please contact, the DCSS Information Security Office at (916) 464-5045 or info.security@dcss.ca.gov

ISO File Library

This application is located on the DCSS LCSA Secure Website. The purpose of this application is to provide an easy and secure means of file/document exchange between DCSS Information Security Office (ISO) and the LCSAs.

Access to ISO File Library Application:

The designated LCSA user(s) will need to request access by contacting the DCSS Statewide Application Service Desk at StatewideApplicationsServiceDesk@dcss.ca.gov. The request requires supervisor approval and it is recommended the LCSA designate no more than 2 individuals who will be authorized to access and upload documents to this ISO File Library.

User instructions: Upload a file/document

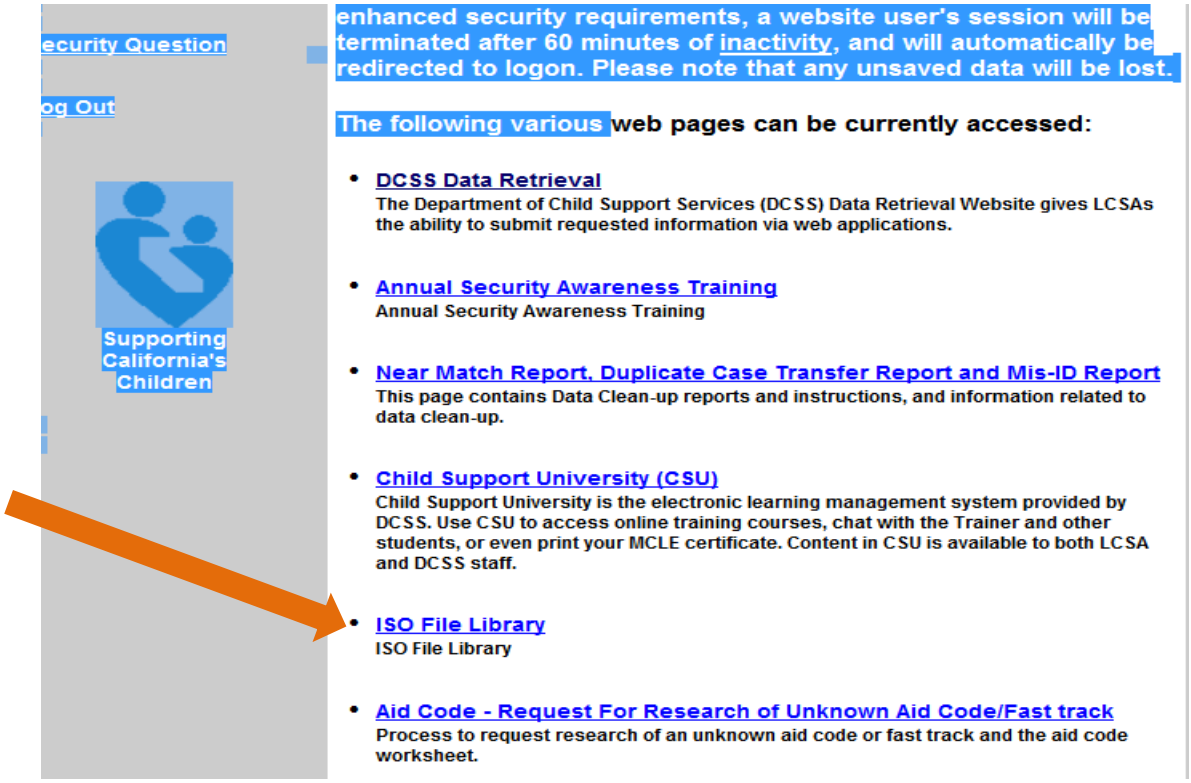
1. Logon to DCSS LCSA Secure Website
2. Select ISO File Library
3. The authorized user(s) will only see their county name listed. County Name cannot be changed.
4. On the Folders pull-down menu select appropriate folder:
    a. BCMP
    b. Compliance
    c. DMV
    d. Miscellaneous
    e. Security Awareness
5. Select the Browse tab and locate the file to be uploaded. Click on Open, when ready to upload. NOTE: file size must not exceed 50 MB
6. Then select the Upload File tab
7. A “File was uploaded successfully!” message will be displayed. You should also see file/document uploaded.
8. This completes the upload process. To upload more files, repeat step 4 – 7.
9. The user has option to delete a file from any of the folders for their county by selecting the file to be deleted and then selecting the Delete tab.

User instructions: Retrieve an uploaded file:

1. Follow steps 1 through 4 listed above.
2. The authorized user(s) selects the file/document to retrieve.
3. You will be prompted to ‘Open’ or ‘Save’.
4. ‘Save and Open’ option will save to the default download location for your PC.

You can upload files to this location for sharing between an LCSA and DCSS Information Security Office. LCSA users can perform these tasks ONLY for their own county.

Step 1: DCSS LCSA Secure Website – Main Page



2: ISO File Library: