Agency Selected Topics

Office Hours Calls

June 2022

Thank you for all your questions and topic submissions!

We truly value your input as our partners.

External Safeguards Training

Q: It would be helpful to get training material on how to get started with safeguards, checklists on things to do, and possibly a frequently asked questions (FAQ) section.

A. Safeguards is looking into developing a training for new points of contact (POC). Until a training is developed, agencies can rely on the following to get started with Safeguards:

Publication 1075

- Provided to all agencies and is available at http://www.irs.gov/uac/Safeguards-Program.
- Publication provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, contractors, or sub-contractors adequately protect the confidentiality of federal tax information (FTI).
- Identifies submission due dates.
- Explains safeguarding processes.

Safeguard Security Report (SSR) is the primary source for agencies to report to IRS on the processes, procedures, and security controls in place, to protect FTI provided in accordance with IRC 6103(p)(4).

- Submitted annually by the agency.
  - Reports all security controls.
  - Due dates for the SSR are in Publication 1075 -Table 4.
- SSRs are living documents that require periodic review, modification, and Plans of Action and Milestones (POA&M) for implementing security controls.
- Describes how the security controls and control enhancements meet Publication 1075 requirements.
- Validated during onsite security control reviews.
- Requires head of agency (HOA) certification and approval.

External Safeguards Training (Continued)

Q: It would be helpful to get training material on how to get started with safeguards, checklists on things to do, and possibly a FAQ questions section.

Safeguards Reviews

- Ensures protection and use of FTI in accordance with statutory and regulatory requirements
- Continuous interaction and onsite reviews conducted every three years or as needed
- Comprises of physical security; system computer security; personnel security; and disclosure awareness
- Onsite review preparation timeframes
  - 90-120 days out make initial contact.
    - Notification letters
    - Secure Agency contact information for coordination
    - Identify concerns
  - 60-90 days out provide agency with information to assist with review
    - Sample logs
    - Publication 1075
    - Request information
  - 60-30 days out review information provided by the agency
    - Review Prep Questionnaire
    - Preliminary Security Evaluation (PSE) document
  - 30-0 days out
    - Finalize agenda
    - Finalize review preparations.
  - Post Review
    - A Safeguards Review Report (SRR) and Corrective Action Plan (CAP) will be issued within 45 days of the closing conference to document the review findings.
    - Requests for corrections to the SRR must be emailed to the SafeguardReports@irs.gov mailbox. The Office of Safeguards will respond with an acknowledgement and a determination.

External Safeguards Training (Continued)

Q: It would be helpful to get training material on how to get started with safeguards, checklists on things to do, and possibly a FAQ questions section.

Resources

- **Safeguards Website** – Contains helpful information such as, Publication 1075, templates, and guidance.
  - Provides internal inspections templates.
  - Provides guidance for updating Safeguards through the notification process.
  - Provides frequently asked questions (FAQs) on various topics.
- **Safeguards Mailbox** – Used for questions you may have for the Office of Safeguards relative to safeguarding requirements and Publication 1075.
  - Can be used to submit updates.
  - Can be used to ask questions, if not covered under the FAQs.

Exhibit 7 Language

Q. What is the expectation for the new Exhibit 7? Comparing the previous version of Exhibit 7 and the new version, you do not see this language in the previous version:
"(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI".

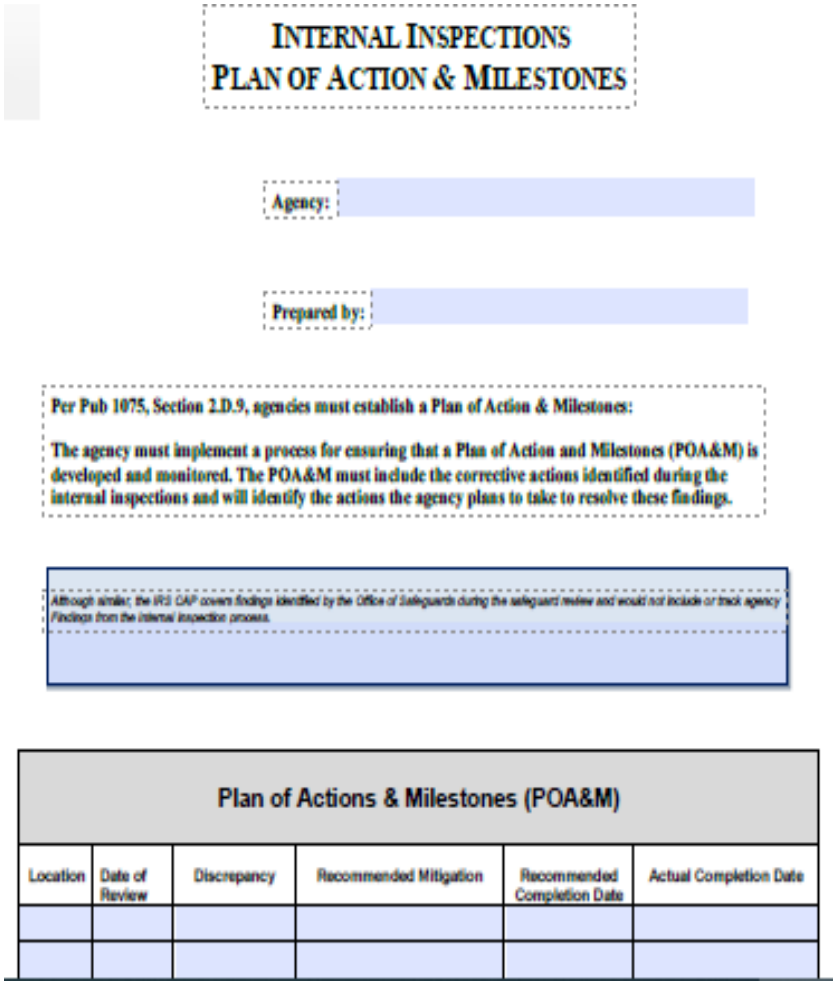
A. All contractors and sub-contractors need to have exhibit 7 language, without modification.

Plan of Action and Milestones (POA&M)

Q. Could you provide a detailed explanation of what is expected to be included in a Plan of Action and Milestones? Examples and/or a template would be very much appreciated.

A. The POA&M should have CAP findings, internal inspection findings, and anything else the agency is tracking for remediation (e.g., vulnerability scan results). “The POA&M must comprise of an all-inclusive tool or document for the agency to track vulnerabilities identified by the self-assessments, internal inspections, external audits and any other vulnerabilities identified for information systems that receive, process, store, access, protect and/or transmit FTI.” – Publication 1075 4.4 Assessment, Authorization and monitoring CA-5

Examples of the POA&M are found on Internal Inspections Reports



INTERNAL INSPECTIONS
PLAN OF ACTION & MILESTONES

Agency:

Prepared by:

Per Pub 1075, Section 2.D.9, agencies must establish a Plan of Action & Milestones:

The agency must implement a process for ensuring that a Plan of Action and Milestones (POA&M) is developed and monitored. The POA&M must include the corrective actions identified during the internal inspections and will identify the actions the agency plans to take to resolve these findings.

Although similar, the IRS CAP covers findings identified by the Office of Safeguards during the safeguard review and would not include or track agency findings from the internal inspection process.

Plan of Actions & Milestones (POA&M)					
Location	Date of Review	Discrepancy	Recommended Mitigation	Recommended Completion Date	Actual Completion Date

Securing MFD Hard Drives

Q. Please provide information regarding the type of container/lock that should be used to prevent physical access to the hard disk of Multifunction Devices (MFDs) or High-Volume Printers (HVP)?

A. This is a moderate finding (GENPRNT-17) and has been a requirement in the Printer/MFD/HVP SCSEM. A lock for accessing the Hard Disk Drive (HDD) is not require if the drive is encrypted.

What we are looking for here is a locking mechanism with a key securing the hard drive or the case access to the hard drive.

- Even a drive that cannot be removed but the connectors can be removed is vulnerable.
- See if the vendor makes a lock
- If the vendor does not supply a lock, acquire an aftermarket lock that will secure the drive so that it cannot be accessed.

We will update the SCSEM to state that a lock may not be require if:

- Physical security measures are in place
- The drive is not easily removable
- The drive is encrypted, or if there is zeroization or other strong protection mechanism

IT Nessus/SCSEMs

Q. Will the IRS Office of Safeguards provide Safeguard Computer Security Evaluation Matrix (SCSEMS) and Nessus audit files that are customized for a clustered Oracle database (DB) environment?

A. Our SCSEM development/prioritization is driven by system components we encounter during Safeguards reviews. We currently use the applicable Oracle DB SCSEM for clustered Oracle DBs. We will need to follow up to determine if we:

- Are seeing many clustered Oracle DBs
- Have existing Oracle DB SCSEM requirements/checks that are problematic for clustered DBs

Q. Nessus audit files are currently available for Oracle 19c, will Safeguards provide a SCSEM for Oracle 19c?

A. We have posted Nessus audit files and a SCSEM Oracle (19 RDBMS) on the Safeguards website.

Spillage

Q. Could you please clarify the procedures related to “spillage”? Specifically, when does “spillage” of federal tax information need to be reported to IRS Safeguards?

A. All FTI spills needs to be reported to the IRS Safeguards. The information can be found on page 36 of Publication 1075 in 1.8.2 General.

Information spillage refers to instances where FTI is inadvertently placed on systems that are not authorized to handle FTI or are not part of the agency's intended FTI workflow. Upon discovery, corrective action is required to remove the FTI from the unintended system and ensure there were no unauthorized accesses or disclosures. If no FTI is involved, then there is no need to report the spill to the Office of Safeguards or TIGTA. If the agency cannot show FTI was not involved within that 24-hour period, then the spill will need to be reported to the Office of Safeguards and TIGTA.

Internal Inspections

Q. Our contracted IT staff is currently housed in the same state office as our state personnel. Internal inspections for this state office are conducted every 18 months. Can the contracted IT staff be included in the internal inspections conducted for the state office?

A. Publication 1075 Section 2.D.3 breaks out the following:

- Headquarters office facilities housing FTI and the agency computer facility at least every 18 months
- All contractors and sub-contractors with access to FTI, including a consolidated data center or off-site storage facility: at least every 18 months

Contractors who work at the headquarters or state-run data center would fall under internal inspections every 18 months.

.

Taxpayer First Act (TFA) Section 3002

Q. Request for review of communique on Taxpayer First Act (TFA) Section 3002. Please provide general overview.

A. When an Agency proposes an adverse or disciplinary action the Agency must then notify the impacted taxpayer in writing, including the date of the unauthorized inspection or disclosure of return information by the Agency employee and the taxpayer's rights under IRC section 7431.

A. UNAX or UNAD
B. Data Incident report to Safeguards
C. Adverse or disciplinary action
D. Letter to impacted individual
E. Notify Safeguards when letter sent

Shared Findings

Q. Agencies have noticed, with findings on CAPs that are shared, they will put the same response and Safeguards will sometimes close one CAP and the other remains open. What is the correct way to respond to get the other one closed?

A. Safeguards is aware of this and looking for ways to reduce or eliminate the occurrence. As CAPs come in from different agencies and assigned for review, there is the possibility these are assigned to different reviewers.

A. Identify shared findings in report
B. Assign all CAPs for state to same reviewer
C. Look at ways to consolidate shared finings

Hybrid Review Process

Q: Please provide an update for the following:

i. The status of the hybrid-review model.

ii. Have any changes been made to this review approach?

iii. Can the IRS confirm specific expectations associated with the hybrid-review model?

- The hybrid-review model remains in a pilot status with plans to be implemented as the standard review method going forward.
- Hybrid reviews are two weeks in duration with the first week being IT reviews conducted remotely (Mon-Fri). The data flow is conducted on Monday during this week.
- The onsite review follows the IT week. The duration is Tues – Thurs with the opening on Tues and closing on Thursday
- There are no differences with expectations between the hybrid and onsite reviews.

Note: The Hybrid Review process would be addressed with the agency by the DES assigned the case during the 120-day review preparation process. The DES preparing for the review should be able to address most of the above.

IRS's Information System Security

Q. Our office of Information Technology submits a lot of sensitive information to the Office of Safeguards; how can we be assured that this information is protected since we don't have a contractual or statutory agreement with Safeguards?

A. The Office of Safeguards only places information in authorized information systems per Internal Revenue Manual 10.8.1

- The IRM references applicable laws, federal regulations, Executive Orders, OMB guidance, TDs, NIST Publications, etc. that we must adhere to for data privacy and information (system) security to include: NIST SP 800-37, Federal Information Security Modernization Act of 2014 (FISMA), Treasury Directive 85-01, FedRAMP, FIPS 140.
- Many of these requirements are reflected in Publication 1075.

Telework

Q. Could you have a discussion on the changes in Publication 1075 regarding telework and/or alternate work sites?

2.B.7 Alternate Work Site - If the confidentiality of FTI can be adequately protected, telework sites such as employee's homes or other non-traditional work sites can be used. FTI remains subject to the same safeguard requirements and the highest level of attainable security.

All the requirements of Section 2.B.5, Physical Security of Computers, Electronic and Removable Media, apply to alternate work sites. All computers and mobile devices that contain FTI and reside at an alternate work site must employ encryption mechanisms to ensure that FTI may not be accessed if the computer is lost or stolen.

See Section 2.B.7 Alternate Work Sites If permitted, a policy/procedure must address the security of FTI at alternate work sites. A policy is required even if alternate work sites are prohibited.

- Section 2.B.7, Alternate Work Site, no longer includes requirement for agency inspections of telework locations

Cloud Usage

Q. Please provide clarification on Cloud Usage

A. If properly implemented, Safeguards will consider encryption and (logical) access controls a logical barrier and will allow data types with restrictions (e.g., IRC § 6103 (l)(7), (l)(10)) to move to a cloud environment.

Commercial/public cloud deployments* are acceptable for all agency types/FTI **if** proper access controls are in place to include adequate encryption:

- FIPS 140 validated encryption must be utilized (at rest and in transit)
  - Keys are managed, controlled, and owned by the agency to prevent logical access by the cloud provider

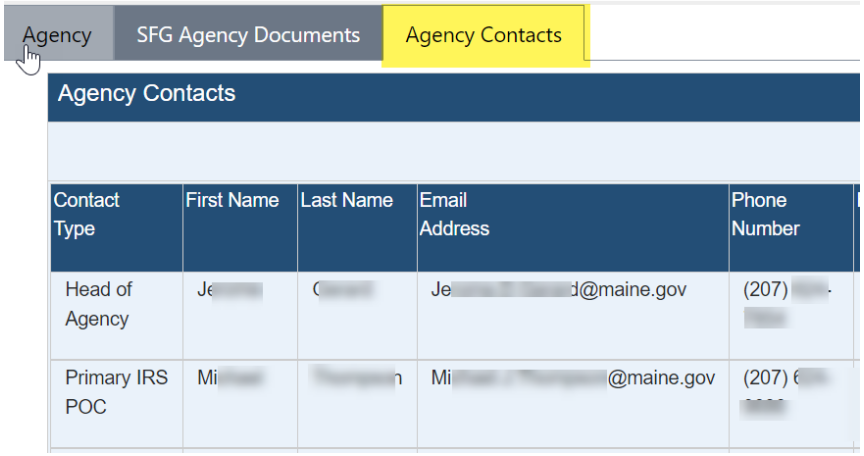
*All cloud service offerings must meet our requirements to include FedRAMP authorized for moderate impact to be acceptable for FTI. FTI must also be geographically restricted to to the US.

Agency Contacts

Q. Who receives the invites for Office Hours Calls?

A. Currently, the invites are sent to the **Primary IRS POC** and **Primary IT POC. S**afeguards receives the POC from the agency on the questionnaire during the review process. In order to keep our POC listing current, we require the agencies to update us with their most up-to-date information. **The POC's may forward the invites to the agency employees who wish to attend the calls.**

We have now migrated to using Microsoft Teams as our tool for hosting the calls. In the past, we used WebEx and Zoom, which limited the number of attendees.



Updated Safeguard Security Report (SSR)

It isn't recommended that agencies copy data from old SSRs into the new template because requirements have changed due to updates in NIST SP 800-53 Rev 5 and IRS Publication1075, which include:

- New controls (e.g., SR-1)
- Changed/updated requirements for some controls (e.g., IA-5's minimum password length went from 8 characters to 14)
- The controls themselves changed due to NIST SP 800-53 updates from revision 4 to 5 (e.g., requirements for AU-8 were split between AU-8 and SC-45)

In many cases the (old) requirement(s) did not go away, they were moved and are covered elsewhere. The notes in NIST SP 800-53 Rev. 5 can shed some light on this:

AU-8	**TIME STAMPS**
	(1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE [Withdrawn: Moved to SC-45(1).]
…	
SC-19	**VOICE OVER INTERNET PROTOCOL**
	[Withdrawn: Technology-specific; addressed as any other technology or protocol.]

Safeguard Security Report (SSR)

- Agencies do not need to copy IRS Responses from their old SSR on to the new template.
- Agencies have the option to submit their 2022 SSR on the new template. 2023 SSRs must use the new template.

Q&A