Office of Privacy,
Governmental Liaison & Disclosure

IRS Safeguards

Office Hours

Topic: Remote Assessments

July 2020

Agenda

- Remote Assessment Plan Overview
- What does a Remote Assessment look like?
- Scheduling Considerations
- Remote Selection Considerations
- Physical Assessment
  - Policy/Procedures, Contracts, Visitor Access Logs, etc.
- IT Assessment
  - MOT, Nessus and Manual SCSEMs
- Effect on Out of Cycle (OOC) Reviews and (p)(7)
- Looking Ahead
- Discussion and Questions

Remote Assessment Plan Overview

- Limiting large group meetings, face-to-face interactions, and travel because of the COVID-19 pandemic has affected the Office of Safeguards on-site security asessments. While Safeguards prefers on-site assessments, we must consider the health and safety of IRS personnel as well as our agency partners when making decisons about in-person assessments.

- Because of COVID-19 circumstances, conducting remote assessments with virtual-ready tools is our best active solution.

- Together, Safeguards and our partner agencies will perform assessments remotely to make sure federal tax information is protected per IRS Publication 1075.

What does a Remote Assessment look like?

IRS Safeguards expectations will remain the same.

- An agency must have appropriate staff available to test all technologies that receive, store, process, transmit or access FTI.

- Safeguards will review your IT environment with Nessus and manual SCSEM testing through WebEx sessions, telephonic interviews and email or SDT document sharing. Safeguards will conduct the physical side of the review through telephonic interviews, as well as email and SDT of policy documents and other requested evidence.

- There will be no portion of a remote assessment that will be conducted in person.

Scheduling Considerations

- If Safeguards postpones a review, the postponement will be based on Safeguards travel restrictions and/or state restrictions.

- For reviews originally scheduled from January through October 1, 2020, Safeguards held outreach sessions with each state agency to gather information on several factors such as the ability to support a remote review, onsite review, current posture of the state in relationship to COVID-19 and agency personnel availability.

- Safeguards will work to limit remote assessments to a one week timeframe.
  - Opening conference, data flow and testing will begin on Monday
  - Testing will continue through Thursday and potentially into Friday
  - Closing conferences will be tentatively scheduled for Friday

Remote Selection Considerations

- Prior to scheduled review dates, Safeguards will notify partner agencies concerning any remote assessments and/or review postponements. Once IRS releases travel restrictions, Safeguards will assess next steps for the assessment schedule for upcoming agencies.
- Remote assessments will be conducted by state whenever possible; however, reviews of individual agencies may also be considered.
- A remote assessment replaces the on-site review in the 3-year review cycle; however, Safeguards will also have to account for individual state agencies that need to be assessed to get the state back on track as a whole.

Physical Assessment

- The physical side of a remote assessment review will be conducted via telephonic interviews with key personnel to discuss the program and processes (e.g. questions on logging, MPS, the movement of FTI at different locations, etc.).
- Policy documents and requested evidence will be submitted via email and/or SDT. For example:
  - Badge policy
  - Alternate Work Site policy
  - Tailgating policy
  - TDS procedures
  - Incident response policy
  - Email/Fax policy
  - Background Investigation policy
  - Disposal/Destruction documents
  - Contracts

Physical Assessment - Continued

Additional documents requested

- SLA
- Internal Inspection reports and Plan
- Internal inspection POA&M
- Disclosure Awareness Training Program
- Visitor Access Logs
- Authorized Access List
- Badge Logs
- Key Logs/Inventories
- Need/Use
- Warning Banners
- FTI logs
- Audit Logs/records
- Access Control Logs

IT Assessment

- **What tools does the agency need to conduct an IT remote assessment?**
  - Each agency should be able to access an IRS initiated WebEx session and be able to share an application over the session.
  - To perform scans, an agency needs an instance of Tenable Nessus, or the ability to install Nessus on agency equipment using a temporary IRS Nessus license, or an agency provided VPN connection to the network to allow use of an IRS instance remotely.
- **What will the dataflow process look like?**
  - Safeguards will conduct the dataflow discussion over WebEx, likely using MS Word as the dataflow will be more of a narrative than the typical diagrams drawn on-site.
- **Are there any technologies that will be exempt from a remote assessment?**
  - Air-gapped/Standalone systems may not be able to be reviewed if the agency cannot remotely access those systems. This will be determined based on each individual agency and system.

IT Assessment - Continued

- The IT scope will be very similar to that of an on-site review. Safeguards will assess all systems that receive, store, process, transmit or access FTI.
- We will conduct remote assessments in a similar manner as a typical on-site review. We will do the following:
  - Review the MOT documents (IT policies and procedures)
  - Perform Nessus scans (automated checks)
  - Walk through the SCSEMs (manual checks) with administrators
- We will review shared technologies/infrastructure only one time and share findings among the agencies as applicable.

Managerial, Operational and Technical (MOT) Review

- We will continue to ask agencies to provide the necessary policy and procedure documentation in advance of the review (using zip file, SDT, secure email) if possible or immediately following the opening conference.
- We will continue to conduct MOT review sessions as part of the IT schedule to walk through any gaps with appropriate agency personnel and give the agency an opportunity to provide additional documentation as needed.

IT Assessment - Continued

Tenable Nessus Automated Scans

- We will continue to scan all technologies in scope for which we have IRS audit files.
- Scans may be conducted using:
  - The agency's/data center's instance of Nessus (Pro, Security Center, etc.)
  - The agency can download Nessus from Tenable on agency equipment and IRS will temporarily provide an IRS license to complete the scans.
  - IRS instance remotely using an agency provided VPN connection to the network
- If the agency is conducting the scans, Safeguards will verify the scan policy is set correctly, ensure the proper audit file is being used and witness scans being run over a WebEx session.
- Safeguards will hold a Nessus prep call as necessary to walk through Nessus scanning, help troubleshoot issues and/or help set up a Nessus instance to ensure scans go smoothly during the review.
- Scanning credentials will need to be provided to either the agency Nessus administrator/POC or to the IRS (if Safeguards is performing the scans).
- The IT schedule will show Nessus scanning with time allotted for completion.
- Systems that are standalone/air-gapped and cannot be scanned will be handled on a case-by-case basis and determinations will be made on how to assess.

IT Assessment - Continued

Safeguard Computer Security Evaluation Matrices (SCSEM)

- We will continue to work with the administrators of the technologies in scope to go through the manual checks.
- Safeguards will use WebEx sessions to “shoulder surf” agency administrators as they share their screens in order verify the necessary configuration settings.
- We will still provide SCSEMs in advance of the review as part of the normal process.
- The IT schedule will show all manual assessments with time allotted to complete the checks.
- It is crucial to identify the agency/data center POCs for these assessments prior to the review so we can schedule the WebEx sessions appropriately.
- We will attach SCSEMs to the WebEx invites so the administrators are familiar with the questions that will be asked during the sessions and can prepare accordingly.

Effect on Out of Cycle Reviews & (p)(7)

- The Out Of Cycle (OOC) program will continue to use risk based methodology to identify agencies that present unacceptable risks to the Safeguards program.

- Safeguards will conduct OOC reviews remotely until the IRS, states and agencies resume normal operation.

Looking Ahead

- Our remote assessment plan is not intended to eliminate on-site reviews. Instead, we have positioned ourselves as a trusted partner to help agencies streamline the review process while maintaining compliance and strengthening security postures within their organization.

- We have no plans to extend or to continue fully remote assessments beyond the COVID-19 crisis. However, should it become necessary, fully remote assessments could be used again in the future.

- As far as individual testing methods, we will analyze lessons learned from remote assessment activities and incorporate enhancements into normal on-site reviews as process improvements.

Questions and Discussion

Please feel free to provide us with topics you are interested in and would like to hear more about in future sessions!