IRS OFFICE OF SAFEGUARDS

OFFICE HOURS

TOPIC: IT SCOPING AND ELECTRONIC DATA FLOW

The IRS Office of Safeguards (Safeguards) hosts Office Hours for agencies to get more information or support on specific topics relevant to the safeguarding process. Office Hours is a forum for agencies to ask questions and interact with subject matter experts.

Topic: IT Scoping and Electronic Data Flow

Date: August 2018

OVERVIEW OF THE SAFEGUARDS REVIEW

Every three years Safeguards conducts an on-site review of each agency that receives federal tax information (FTI) from the IRS. The Safeguards team evaluates the physical and logical controls set up by agencies to protect FTI from loss, breach or misuse. The team tracks FTI from point of receipt through processing, transmission, storage and final disposition. As explained in IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, the review scope includes an in-depth review of logical computer security controls and configuration of an agency's operating systems and telecommunication devices.

IT PRE-REVIEW ACTIVITIES

Safeguards Review Timeline

1. 90 to 120 days before the on-site review, Safeguards informs the agency about the on-site review by sending the agency an official letter.
2. About 75 days before the review, Safeguards sends an email about the preliminary security evaluation (PSE) to the agency. The email includes these materials: PSE form, MOT SCSEM, data flow diagram and Nessus preparation package.
3. About 30 to 60 days before the review, the PSE takes place to discuss systems, platforms and applications with FTI.

The computer security and physical portions of the Safeguards review have two different schedules. The agency can anticipate the IT review schedule about 1 to 2 weeks before the on-site review. This schedule will have proposed, tentative times for the week of the Safeguards review and identify shared devices to limit redundant coordination and assessment.

Personnel Involved in Review Preparation

Personnel responsible for receiving, processing, storing and transmitting FTI should attend the PSE call, including the:

- Information system security officers;
- Agency points of contact responsible for coordinating the IT and physical security portions of the Safeguards review;
- System administrator for Windows and NIX operating systems involved in the FTI flow;
- System programmer/security administrator for mainframe related technologies, such as RACF, ACF2, CA Top Secret and Unisys;
- System developers for FTI-related applications (state or vendor managed);
- Network administrator responsible for day-to-day operation of the LAN/WAN;
- Business process leads or managers to help in the FTI data flow;
- Agency point of contact responsible for conducting Nessus automated testing;
- Data center point of contact when a consolidated data center hosts any FTI systems or technologies.

Involve data center personnel in the Safeguards review process as early as possible. They can help prepare the PSE document, attend the PSE conference call and work closely with the agency to prepare for the on-site review. Share the on-site review schedule with data center personnel and include them on all preparation calls.

IT Scoping

The computer security review team will review:

- Agency data flow.
- Applications (web software, database).
- Underlying hosts, such as mainframe, Windows, UNIX. When using virtual hosts hypervisors may be brought into scope as well as any backend storage devices.
- Business functions used by the agency for FTI, including printing processes, fax systems, email systems, scan applications.
- Access to FTI, including direct end user access and privileged access to FTI systems and technologies. This includes checking end users and administrators' work stations and laptops.
- Networking systems including:
    - Perimeter/edge firewalls protecting any FTI enclave or environment regardless of the encryption level.
    - Remote access solutions used by end users and administrators.
    - Secured wireless networks used to access FTI systems or manage FTI infrastructure.
    - Site-to-site tunnels and network connections to third-party sites or vendors.

    - Core routing devices. If FTI is fully encrypted while traversing an internal network, the Safeguards team can remove the core router from the agency's proposed IT scope.
- County/field and third-party support and access.
    - The agency should identify third parties in the PSE form and discuss them on the initial PSE call. During initial discussions, the Safeguards team will request a mini-PSE call and schedule a short, one-hour meeting between the IRS, agency and third party. During mini-PSE calls, the Safeguard team will discuss and decide business use as well as IT data flow.

Outstanding Items and Post-PSE Communication

The assigned IT agency lead is responsible for reviewing notes taken during the PSE call and sending a list of any outstanding items and questions to the designated agency point of contact. Once the agency answers majority (if not all) questions, the IT agency lead will send a proposed IT scope, SCSEMs for conducting the assessment and Nessus prep material with platforms for assessing with Nessus on site.

The Office of Safeguards will coordinate logistics with the agency.

Proposed IT Review Schedule

The IT state lead will create a proposed IT review schedule to make sure any shared devices are identified and scheduled accordingly. The lead will share the schedule with the agency point of contact 1 to 2 weeks before an on-site review.

- A sample review schedule will be included as part of the WebEx.

SAFEGUARD SECURITY REPORT

It's important to keep an accurate flow of FTI in the Safeguards Security Report (SSR), *Section 9.2 Electronic Flow.* Agencies should attach a description of the flow of FTI (physical or electronic) within their infrastructure and IT systems to their SSR submission.

For each device described in the flow that stores, transmit, processes, or receives FTI, agencies need to identify the following:

- Platform, such as mainframe, Windows, Unix/Linux, router, switch, firewall;
    - If mainframe, number of production LPARs with FTI, security software (examples: RACF, ACF2)
    - If not mainframe, number of production servers or workstations that store or access FTI
- Operating system, such as z/OS v2.2, Windows 2012, Solaris 10, IOS;
- Application software, including commercial off -the- shelf or custom, used to access FTI and
- Software used to retrieve FTI, such as SDT, CyberFusion, MFT.