Office of Privacy,
Governmental Liaison & Disclosure

IRS Safeguards

Office Hours

Topic: Safeguards Review IT Scoping

August 2018

Agenda

- IT Review Timeline
- Review Preparation
- IT Scoping
- Sample IT Review Schedule
- Post-Preliminary Security Evaluation (PSE) Activities

IT PSE Review Timeline

~90 - 120 Days Prior to review
Review Notification Letter Issued

~75 Days Prior to Review
Preliminary Security Evaluation Call Outreach Conducted

~30 - 60 Days Prior to Review
Preliminary Security Evaluation Call Held

- *The computer security and physical portions of the Safeguards review will have two different review schedules.*
- *Agencies may anticipate the IT review schedule approximately 1-2 weeks prior to the onsite review. This will include proposed, tentative times for the week of the Safeguards review and will identify shared devices to reduce redundant coordination and assessment during the onsite review*

Personnel Involved in Review Preparation

Personnel that have responsibilities involving the IT operating environment for receiving, processing, storing and/or transmitting Federal Tax Information (FTI) should attend the PSE call:

- Information System Security Officer(s) responsible for secure operation of the FTI system.
- Agency POC responsible for coordinating the IT security portion of the Safeguards Review.
- Agency POC responsible for coordinating the physical security portion of the Safeguards Review.
- System administrator for Windows and/or *NIX (where applicable) Operating Systems involved in the FTI flow.
- System programmer/security administrator for mainframe related technologies (e.g. 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 management to assist in the FTI data flow.
- Agency POC responsible for conducting the Nessus automated testing.
- Data center POC when a consolidated data center is used to host any FTI systems or technologies.*

*If applicable, data center personnel should be involved with the Safeguards review process as early as possible. This includes assisting with the preparation of the PSE document, attending the PSE conference call and working closely with the agency to prepare for the onsite review. It is recommended that agencies share the onsite review schedule with data center personnel as well as work to include them on all preparation calls.

Onsite Review: Assessment Capabilities and Scope Overview

All IT systems used to process, store, receive and/or transmit FTI are included within an agency’s scope

- **Agency**
  - Headquarters
  - Consolidated Data Center
  - Hosted Data Center
  - Field Offices
- **Third-Party Providers**
  - Collection Agencies
  - Call Centers
  - Print Shops
  - Cloud Providers

NETWORK / INFRASTRUCTURE

Network Assessment
Firewalls
Remote Access Solutions
Wireless
Core Router/Switch
Hypervisor and Storage

APPLICATION

Application (e.g., RSI, Teradata, GenTax)
Web Server
Database
Warehouse
Operating System(s)/Host

ACCESS

Operating System(s) for end user and admins
Mobile Devices
VDI

SERVICES

Cloud
VoIP Infrastructure
Call Storage
MFD / HVP
Print Application Software
Operating System

Including Full Version Information

Agencies are requested to provide sufficient device information during the review preparation period. Please provide the make, model and firmware of each technology as applicable. Some examples are provided below as guidance:

- Windows 2008(R2) or Windows 2012(R2)
    - Please include if the server is Windows 2008, 2008R2, 2012 or 2012R2.
- Linux/Unix Variants
    - Please include full version (e.g – Red Hat Linux 5.11, AIX 7.1, Solaris 11.1).
- SQL Server
    - Please include version and build (e.g – SQL Server 2008R2 – Build 10.50.6560.0).
- Oracle Databases
    - Please include full version (e.g – Oracle 12c – version 12.1.0.2).

Including Full Version Information (Cont.)

- VMWare ESXi
  - Please include the full version information for VMWare and Vsphere (if used) (e.g – VMWare ESXi 6.0.0 / VSphere 6.5)
- Networking Devices
  - Please include make, model and full version (e.g – Cisco 6509-E IOS 15.1(2)SY10, Cisco Nexus 7000 NX-OS 8.3(1), Pulse Secure PSA5000 v8.3, Fortinet Fortigate 500D FortiOS 5.6.0).
- Storage Area Network (SAN)
  - Please include make, model and full version (e.g – PureStorage FA-M70R2 Purity v4.8.11, EMC Isilon X400/X410 SAN - OneFS v8.0.0.4).
- Printers
  - Please include make, model of all networked, multi-function or high volume printing devices involved in FTI (e.g – Xerox Nuvera).

IT Scoping

- The computer security review team will review the entire electronic flow of FTI within all IT equipment and network devices that process, receive, store, transmit and/or maintain the data.

- The data flow diagram will be used for the onsite Safeguards review but may also be used to maintain an accurate flow of FTI in the Safeguards Security Report (SSR), *Section 9.2 Electronic Flow*. It is recommended that agencies attach a representation of the flow of FTI (physical or electronic) within the agency's infrastructure and IT systems to their SSR submission.

IT Scoping: Networking

The Office of Safeguards tests network protections and infrastructure of entities receiving, creating or accessing electronic FTI

	Systems for Assessment				
FTI Processing Scenario	Network Assessment	External Firewall(s)	Remote Access Solution(s)	Router/ Switch*	Wireless**
Receives electronic FTI	Yes	Yes	Yes	Yes	Yes
Creates electronic FTI (i.e.,scanning or call recording)	Yes	Yes	Yes	Yes	Yes
Standalone FTI Processing	Yes	No	No	No	No
Accesses electronic FTI from non-agency network	No	Yes	No	No	No
Accesses electronic FTI via Agency managed VDI	No	No	No	No	No

🟦 Agency or Third Party 🟩 Third Party

* Router/Switch included only if FTI is not encrypted while traversing internal network

** Wireless included in scope when there is a secure/trusted wireless network

IT Scoping: Virtual Desktop Infrastructure (VDI)

Agencies have increased utilization of VDI solutions to grant access to FTI and FTI-processing systems

- Presents complete virtual desktops to client machines
- Permits agency control of VDI images (e.g., A/V)
- Secures covert channels (e.g., copy/paste, print capabilities)

SCSEM Library for VDI Infrastructure	
• Remote Access Capabilities	• VPN
• VDI Manager, Gateway and Hosting Servers	• Operating System(s) flavor and version
• Desktop Images	• Operating System(s) flavor and version

Third-parties accessing FTI systems using agency-managed VDI solutions will NOT be included in the IT scope of a Safeguards review

VDI Requirements: External Information Systems

Publication 1075

Section 9.4.13: Virtual Desktop Infrastructure

- Strong boundary protections enforcing access control
- Limit access to only approved clients
- Harden systems per Publication 1075 requirements using Safeguards SCSEMs
- Limit access to the VDI environment based on least privilege
- Establish a secure baseline for virtual desktop images
- Require multi-factor authentication for remote access
- Enable auditing on all aspects of the system and review audit logs weekly
- Encrypt all connections where FTI traverses

IT Scoping: Application

Systems within Review Scope

- Application
- Web Server Software (e.g., Apache, IIS)
- DBMS (e.g., SQL, Oracle, DB2)
- Mainframe Security Software (if applicable) (e.g., RACF, Top Secret, ACF2)
- Underlying operating system(s) of Web, App and DB Servers (e.g., Windows Server, RHEL, AIX)
- Workstation operating systems for end users and admins (e.g., Windows 7, MacOS X, Windows 10)
- Hypervisor and virtual storage (if applicable) (e.g., VMWare ESXi, IBM XIV)

IT Scoping: Call Center

Systems within Review Scope

- Network infrastructure and remote access
- Call Manager (e.g., Cisco, Avaya) and Call Recording (e.g., Calabrio)
- Underlying operating system(s) of Call Recording System (e.g., Windows Server, RHEL, AIX)
- Call Storage (e.g., EMC SAN, IBM XIV)
- Workstation operating system(s) of Call Agents and Admins (e.g., Windows 7, MacOS X, Windows 10)
- Hypervisor (if applicable) (e.g., VMWare ESXi)

IT Scoping: Print Shop

Systems within Review Scope

- Network infrastructure and remote access
- High Volume Printer and Print Software Application
- Underlying operating system(s) of File Transfer and Processing/Print Servers (e.g., Windows Server, RHEL, AIX)
- Workstation operating system(s) of Printer Operators and Admins (e.g., Windows 7, MacOS X, Windows 10)
- Hypervisor and virtual storage (if applicable) (e.g., VMWare ESXi, IBM XIV)

IT Scoping: Cloud vs. Virtual

Safeguards uses criteria to determine whether a technical solution is in a Cloud environment or is within a Virtual Environment

If cloud, Safeguards will assess:

- Agency workstations
- Cloud

Post-PSE Activities

- The IT Agency Lead will follow up with the Agency POC(s) after the initial PSE call with any outstanding items and/or questions.
- Upon clarification of all questions, the agency can anticipate communication including:
  - Proposed IT Scope
  - SCSEMs that will be used during the onsite assessment
  - Nessus Preparation Material along with a list of platforms that will be tested with Nessus

Sample IT Review Schedule

A proposed IT review schedule will be created by the IT State Lead to ensure any shared devices are identified and scheduled accordingly. The schedules will be shared with the Agency POC 1-2 weeks prior to an onsite review.

Agency Opening	Agency Opening (Obtain MOT documentation)	Juniper Pulse v8.1 VPN** (Need VPN / remote access admin)
		Juniper SRX 650/3400 Firewall** (Need firewall admin)
Start Nessus Scans	Start MOT (Offline review - POC not required at this time)	Network Assessment (Need networking admins and security personnel)
Nessus Scans and Windows Manuals (08R2) (Need Top Level Admin Credentials for All, i.e. sudo or root, domain or local admin) RHEL 5.11 (App/Web/DB Hosts) Windows 2008 R2 (Jump Server) VMWare ESXi 6 (Hypervisor) Oracle 11.2.0.4 (Database)	RHEL (Manuals - and validate extended support, if applicable)** (Need RHEL Admin)	Application** (Need App developers -- confirm critical with Oracle weblogic and Java 6)

Department of the Treasury

Internal Revenue Service

www.irs.gov

IRS Office of Safeguards

www.irs.gov/uac/Safeguards-Program