OFFICE HOURS CALLS

Questions and Answers
March 2022

Subject: Top Technical Inquiries (TI)

Meetings:

Tuesday, March 15, 2022, at 1 p.m. ET (DOR) and 3 p.m. ET (FED/AG/SWA/DOT)

Thursday, March 17, 2022, at 1 p.m. (HS/ACA) ET and 3 p.m. ET (CS)

IT Q & A

1. **Can you please confirm that Live Data Test Request (DTR) notifications are needed for any nonproduction environment? This includes Disaster Recovery (DR), is that correct?**
    a. Yes, the DTR is required for any preproduction environment. DR sites should be considered production, not preproduction. They're governed under the contingency planning (per National Institute of Standards & Technology (NIST) 800-53 and Publication 1075 controls).

2. **Is the Chief Information Security Officer (CISO) certification the same as the Head of Agency (HOA) certification, for decommissioned software or hardware?**
    a. Per IRS Publication 1075, Section 2.E.5.1, either the chief information security officer or the head of agency can sign a certification to document and close findings that no longer apply to the agency's handling of federal tax information.

3. **An agency received IRS responses to its Corrective Action Plan (CAP) that an item wasn't closed due to missing documentation, but it was provided. Is there a problem with putting documentation into subfolders by primary finding?**
    a. Occasionally there can be issues with secure data transfer. If you have questions about CAP responses, you can open a technical inquiry by emailing SafeguardReports@irs.gov.

4. **Will there be a new Safeguard Computer Security Evaluation Matrix (SCSEM) doc for privacy, or will privacy control audits be in the Management Operational Technical (MOT) controls?**
    We don't intend on adding in-depth security or privacy controls to the MOT. Either the disclosure enforcement specialist or IT team will handle this but there is no plan to have a privacy specific SCSEM. Multiple controls that aren't strictly privacy related are already covered in the MOT SCSEM (e.g., AC-1, AT-4, IR-8, PL-4, SA-1, SA-4, SI-1). Other controls are similarly covered in other SCSEMs (e.g., SA-9 via the cloud SCSEM). Additional checks will need to be developed for the PII Processing and Transparency (PT) family of controls, we don't anticipate this will be part of the MOT or cybersecurity checks.
5. **Are there any plans to move away from Excel spreadsheets for the CAP?**
    a. We don't have any plans to move away from using Excel spreadsheets.

6. **Can CISO sign 45-day, LDT and cloud notifications?**
    a. Publication 1075 (Rev. 11-2021) allows the head of agency to delegate signature authority to another individual. See Publication 1075, Section 2.E.2.

7. **For CAPs, we were asked to submit a memo signed by the head of the agency acknowledging that the findings had been remediated. We combined all findings into a single table and submitted this once with our packet but referenced the file multiple times. Is this acceptable, or is there a preference for an individual memo?**
    a. You can have a single memo or letter that addresses multiple findings (e.g., via table). In the CAP, refer to the memo in each of the responses and findings.

8. **We field technical findings from different agencies since we manage the IT infrastructure. As a result, we provide responses to the agencies. Some of our responses are accepted by most reviewers but not all. Is there a plan underway to prevent these inconsistencies for future filings?**
    a. We don't have a specific plan to address this issue yet but are aware of the concern. We're looking at potential process changes and tools that will give us a more holistic view toward better visibility and traceability to address these issues. As a reminder, significant or critical findings require specific evidence (e.g., screen shots) for closure. Moderate and limited findings only need a detailed narrative for closure.

9. **What are the requirements for FedRAMP acceptance?**
    a. The full listing of Safeguards' cloud requirements are in Publication 1075 or on the Safeguards website. These include data isolation, data encryption, FIPS 140 compliance, FedRAMP authorization, keeping federal tax information (FTI) in the U.S., support for "on shore" data and multifactor authentication. Safeguards doesn't manage the FedRAMP program. FedRAMP authorization is **a** requirement but not the only requirement for FTI in the cloud.

10. **Is 7-zip compatible if you configure it correctly to output zip files?**
    a. It's compatible, but the concern is that 7-zip hasn't gone through the Federal Information Processing Standards (FIPS) 140 validation process. Safeguards is not able to open any .7z files and Pub 1075 says it should be a zip file (.zip/.zipx), not 7-zip file.

11. **Can you clarify whether the 7-zip software cannot be used at all or just that archive files using the .7z file extension are not acceptable?**
    a. Encryption to protect federal government information needs to be done with FIPS validated cryptographed modules.

12. **You mention 7-zip cannot be used with encryption because the IRS doesn't use 7-zip. Not following this since 7-zip can also create encrypted .zip files using the advanced encryption standard encryption. Can we still use 7-zip files with encryption?**
    a. The 7-zip's cryptographic modules haven't been evaluated under FIPS 140. If they've been validated under the certification program, please send the validation certificate to

us. If it's not FIPS 140 validated, then it's not adequate for protecting federal information.

13. **We split our CAP to 25 emails (less than 10 MB), yet it is failing to send. We used 7-zip but with .zip extension, and it still isn't successful. It seems that irrespective of .zip extension, 7-zip archived files aren't working.**
    a. We'll follow up to figure out the issue with size limits or error messaging. Email SafeguardReports@irs.gov if you have an issue with your encryption. If you're encountering issues, please provide the following information so we can troubleshoot:
    - Originator's email (From line)
    - IRS email address(es) that should have received the email(s) (To/CC lines)
    - Date/time (and time zone) email was sent (e.g., 4/25/2022 12:27pm ET)
    - Subject line of the email
    - File(s) attached to the email
        - Files name/extension (e.g., 2022SSR.zip, 20221stCAP.xlsx)
        - Size
    - Were they encrypted (e.g., passworded zip file, passworded MS Word document)?
    - Were the emails themselves encrypted (e.g., S/MIME, PGP, OME)?
    - Any error messages/bounce back emails the agency received, or if there was no response from the email

14. **Can you clarify what encryption requirements aren't met with 7-zip?**
    a. The 7-zip tool uses AES, which is a FIPS/NIST standard. But 7-zip's implementation of that standard hasn't been validated to make sure it was properly done.

15. **Is it correct that offices cannot use 7-zip to securely send encrypted FTI data? Our offices use 7-zip to send data. Is this not an approved application to use if we have FTI in a file?**
    a. The 7-zip tool is not an approved Safeguards application, but we're not restricting agencies from using it. If an agency uses the .7z extension instead of the .zip(x) extension, the document will not make it through the Safeguards firewall. The agency must use .zip(x) extension. Encryption with 7-zip hasn't been validated to the FIPS 140 standard, so it isn't adequate for protecting federal information.

16. **I've attempted to send .zip files but it seems that there's a very small size limit for the file. Is that true? If so, what's the size limit?**
    a. There's a size limit of 25mb. It's always best to compress before encrypting to increase the output of the files. If problems arise, we'll follow up with an agency to troubleshoot the issue. then we'll follow up with our IT department to get the problem resolved.

17. **Does AES 256 allow for FIPS compliancy?**
    a. AES256 is a NIST standard. Compliance with FIPS 140 demonstrates the standard is correctly implemented in a specific product/component. A list of validated modules is on the NIST cryptographic module validation site.

18. **Must all internet transmissions use FIPS validated cryptography or just be FIPS compliant as the presentation shows?**
    a. FIPS validated and FIPS compliant are two separate things. FIPS validated means that a product has undergone and passed conformance testing via a national laboratory. FIPS compliant means some component has been tested in terms of validated cryptography. The product needs to be FIPS validated in terms of transmitting and encrypting documents. A list of validated modules can be found on the NIST cryptographic module validation site.

19. **Does the IRS approve the cloud notices?**
    a. The IRS accepts cloud notifications per IRS Publication 1075, Table 6. The IRS will only accept cloud services offerings that are FedRAMP authorized and meet other requirements in IRS Publication 1075, Section 2.E.6.1.

20. **Is it possible to have on-site audit findings in the NIST OSCAL/XML format in addition to the standard Excel file that's sent out?**
    a. We're not planning on doing this. A lot of work goes into the methodology for formatting SCSEMS. We want to move away from Excel and create a system to automate some of the test cases.

21. **Will a cloud request be rejected if it doesn't meet FedRAMP requirements?**
    a. Per Publication 1075, cloud service offerings must be FedRAMP authorized, so the cloud notification would not be acceptable. FedRAMP authorization means a third-party assessing organization (3PAO) has assessed it, and a 3PAO continues to assess it to maintain their FedRAMP authorization. This gives us a reasonable level of assurance that the CSO is operating as intended. Other requirements in IRS Publication 1075 2.E.6.1 beyond FedRAMP authorization need to be met for us to accept the notification.

22. **What are the possible end states of a 45-day notification; "Accepted" and "Not Accepted"?**
    a. A 45-day notification is for cloud computing, disclosure to a contractor, redisclosure to a subcontractor, FTI in tax modeling and FTI in a preproduction environment ("Live Data Test Request"). Cloud computing and disclosure to a contractor will be accepted or denied. All others will be approved or denied. The responses are binary, approval/acceptance or denial depending on the type of notification.

23. **Do you consider Cloud Services Providers (CSP) contractors (e.g., AWS)? CSPs are hesitant to modify Exhibit 7 language in the contract or Service Level Agreement (SLA). Does the IRS have any guidance?**
    a. Yes, CSPs are considered contractors. If they possess the data, they still need to have Exhibit 7 language in the contract. CSPs should be made aware that they need to have Exhibit 7 language in the contract or SLA.

24. **Does the exact Exhibit 7 language need to be in the SLA memorandum of understanding, or can the SLA/MOU simply refer to Publication 1075 - Exhibit 7?**

a. It should not simply refer to Pub 1075, Exhibit 7. The language needs to be in the contract or SLA.

25. **Is there a list of vendors who don't have an issue with adding Exhibit 7 language?**

a. The IRS will not endorse a specific commercial vendor and cannot recommend a vendor. The Office of Safeguards frequently accepts the CSOs listed on FedRAMP's marketplace..

26. **Do our contracts need Exhibit 7 contract language contained in the 11-2021 revision of Publication 1075? Our contractors have the previous version of the language.**

a. All FTI contracts must have Exhibit 7 language. When the contract is updated, we'll expect to see language from the 11-2021 revision of Publication 1075. Please make those updates in the next contract renewal.

27. **If we don't want to pay for third party encryption keys, can we use WinSCP to self-generate AES encryption keys for the Secure File Transfer Protocol (SFTP) or Secure Data Transfer (SDT) channel with the IRS?**

a. We're unsure if this will work with SDT. The agency may reach out to our SDT team mailbox - it-uns.enterprise.service.desk@irs.gov - and include the following:

- SDT agency code (#####)
- Question or issue
- IRS file name
- Requestor's name and contact Info

Just because a product uses AES 256, that doesn't mean it's been certified under FIPS 140 (Cryptographic Module Validation Program). Please visit the NIST website for a list of validated modules.

28. **The IRS Safeguards program is established to identify risks and then track those risks until mitigation. The risks are rated in priority as well. Why are the IRS on-site, internal inspections and Safeguard Security Report (SSR) annual review not considered a risk assessment for CAP MOT H.1.1?**

a. The IRS is looking at risk regarding FTI. We don't have as much of an up-to-date view as the agencies do. Also, doing an SSR annual review is not considered a risk assessment. The SSR is assessing the security plan of the agency. It outlines how the agency is attempting to keep risk at an acceptable level, not evaluate if risk is at an acceptable level. Safeguards is acting as the information owner. We help determine risk tolerance for FTI. Internally, agencies should look at overall risk for their information systems and risk to their mission. Find more information in NIST SP 800-53R5 under RA-3 and NIST SP 800-30r1.

29. **Can we submit other federal assessments on the same system as a risk assessment?**

a. No. Agencies need to perform their own risk assessments. They can include other compliance requirements beyond Pub 1075 (e.g., CJIS, SSA). The IRS is acting as the information owner for FTI; other federal agencies may not consider risk to FTI the same way we do.

30. **Can security assessments and internal audits be part of risk assessments?**
    a. Yes, they should be part of risk assessments.

31. **What is the only acceptable scenario for contractors to enter a data center without an escort? (i.e. a vendor who works for another non-FTI state agency).**
    a. If the vendor is in a space with IT assets that have FTI on them, two barriers protect FTI. A badged employee needs to escort people to a space or cage where data is locked. As soon as the person goes through the door, someone needs to monitor them around FTI.

32. **What is the ETA for the SCSEM which reflects new Publication 1075 requirements?**
    a. The SCSEMs are being reviewed now. Safeguards is expecting to get them out within the next couple of months. If anything changes, we'll provide updates.

33. **Is there an ETA for the new cloud guidance that Steve Matteson talked about on 8 March 2022 during the Safeguards call?**
    a. We're still working on publishing this guidance. While talking with vendors and management, we've learned new information that we're still working through. Once we get everything ironed out, we'll publish the new guidance.

Non-IT Q & A

34. **May we receive copies of the PowerPoint slides?**
    a. Yes. After all calls from this week, everyone will receive a copy of the presentation and the questions and answers in six to eight weeks.

35. **Regarding the 18-month Data Center Inspection Questionnaire, we use a version from 2001. Are we going to see an updated version for our next data center inspection in 18 or so months?**
    a. The most recent documents are on the Safeguards site.

36. **When will the contractor's worksheets be sent to the states?**
    a. We have several individuals working on the TFA project and will have an answer for agencies during the 2023 first quarter Office Hours Call.

37. **Taxpayers First Act (TFA) for a state-owned data center with contractors- Do we need to complete the TFA process (as state-owned data centers are excluded)?**
    a. A state-owned data center would fall under internal inspection. The contractors would be part of that inspection as long as they were only accessing FTI at that facility.