OFFICE HOURS CALLS

Questions and Answers
June 2022

Subject: Agency Selected Topics

Background: The format for the third quarter calls was slightly different from previous calls. The Office of Safeguards solicited the partnering agencies for questions and topics. You'll find the submissions and answers in the PowerPoint presentation link associated with the June 2022 Office Hours Calls.

Meetings:

Tuesday, June 14, 2022, at 1 p.m. ET (DOR) and 3 p.m. ET (AG/DOT/FED/SWA)

Thursday, June 16, 2022, at 1 p.m. ET (ACA/FFM/HS/SBM) ET and 3 p.m. ET (CS)

IT Q & A

1. **Since the Safeguard Computer Security Evaluation Matrix (SCSEM) was just updated, is there something that tells us which test cases were added/deleted?**
    a. Not explicitly. Some test cases weren't deleted, just updated. We're working on making the change logs accessible.

2. **If the agency has a plan to migrate to a cloud solution, as mentioned in the CAP, does that count as a notification, or does the agency need to submit a formal 45-day notification?**
    a. The agency needs to submit a formal 45-day notification.

3. **Is it possible to receive an unlocked Safeguard Security Report (SSR) template?**
    a. The form is automated and therefore locked so it cannot be edited. The agency will also receive an unlocked version to work with when preparing for the response. The locked version must be what is returned to Safeguards.

4. **Many agencies are still transitioning to Rev. 5 requirements. A large number of changes in the new Publication 1075 are aligned with Rev. 5, meaning a number of new controls are not yet implemented. When the next SSR is submitted in January 2023, will the IRS understand that some agencies will not have met the requirements of the new publication?**
    a. Safeguards started testing to new publication standards in June 2022. We'll identify deficiencies accordingly, and you should track them in your POA&M.

5. **Can existing Oracle Database SCSEMs be amended to include variance for clusters if a separate cluster DB SCSEM is not forthcoming?**
    a. If we identify specific tests or configurations that are causing the findings, then we'll look into adding a SCSEM note for specific clusters. If you have any questions on findings, please contact SafeguardReports@irs.gov.

6. **What is the expectation for internal inspection if data is hosted at cloud service provider (CSP) (e.g., AWS, Azure, etc.)?**
    a. We don't expect an internal inspection or on-site review for CSP because that's covered by the Federal Risk and Authorization Management Program (FEDRAMP). However, there is a shared security responsibility model when using CSPs. CSPs and agencies both assume important security roles and responsibilities to ensure FTI data is protected within cloud environments. CSPs must use the customer responsibility matrix (CRM) to describe the specific elements of each control where the responsibility lies with the agency (customer).

7. **Regarding spillage, do we report incidents no less than 24 hours or should it be no more than 24 hours?**
    a. Report all incidents immediately but no later than 24 hours after identifying a possible issue involving federal tax information. Report incidents to the appropriate special agent-in-charge, Treasury Inspector General for Tax Administration (TIGTA), and the Internal Revenue Service Office of Safeguards.

8. **Will an Ubuntu Server SCSEM be created? The Debian does not accurately match Ubuntu.**
    a. Use the generic Unix/Linux SCSEM to assess Ubuntu for now. Safeguards will determine if the Ubuntu SCSEM is required at a later date.

9. **If we're using a newer version of a software with an existing SCSEM, do we use the generic one or the closest related SCSEM? (e.g., IBM DB11; Do we use DB10 SCSEM or generic DB?)**
    a. Use the SCSEM for the older version. If you're having a hard time, you can always check out CIS benchmarks and/or DISA STIGs.

10. **Is the IRS using Tenable-Nessus for audits after 2022? Our state agency is moving to Qualys effective 08/31/2022. Evidently, it will take an extreme effort for our IT department to enable IRS Tenable - Nessus licenses for IRS audits after 2022.**
    a. Currently, Safeguards only uses Tenable Nessus for reviews. If an agency or contractor does not have Nessus, IRS provides a Nessus license to be installed on the agency/contractor workstation or server to perform the scanning.

11. **If a CSP doesn't have authorized access to FTI, is Exhibit 7 language required?**
    a. Cloud service providers need Exhibit 7 language because they store FTI.

12. **Does the IRS send all FTI data (work files) to states using required encryption rates?**
    a. Federal Information Processing Standards (FIPS) are governmentwide. The IRS has policies and some technical restrictions that require us to encrypt sensitive

information that’s transmitted, which includes email. Safeguards doesn't share FTI. If you have a specific question or concern regarding noncompliant transmission from the IRS, we’ll escalate the issue to the correct POC/office.

<u>Non-IT Q & A</u>

13. **What is the date of the next Office Hours call?**
    a. We’ll hold fourth quarter Office Hours calls August 30 and September 1, 2022.

14. **Will the slide deck be shared after the meeting?**
    a. Yes. Everyone will receive the presentation and questions and answers in six to eight weeks. We’ll also post both documents to the Safeguards page on IRS.gov.

15. **Is there a place we can look to in advance to know what the Office Hours call subject(s) will be, so we can make sure we include stakeholders that may have an interest? I realize this call was a bit unique.**
    a. No. We announce the topics in the invitations to the calls.

16. **Recently, we've had some issues getting in contact with TIGTA in reporting issues. The regional contact number we had no longer responds. The web address in Publication 1075 does not provide contact information. The TIGTA hotline number refers us to the TIGTA website to submit issues. TIGTA responded to our website submission indicating that state issues are outside of their jurisdiction. Could you please provide guidance?**
    a. Section 1.8.2 in Publication 1075 has TIGTA information, which includes the web address, hotline number and mailing address. Safeguards is working with TIGTA to correct any confusion.

17. **SSR section 3.1.1 Disclosure to Contractors states:**
    “For this section (3.1), contractors are personnel/entities supporting the agency for compensation, not government employees.”

    We require our non-child support government employees supporting our child support program (IV-D) to enter into contract with us before disclosing FTI. For example, a shared employee processing mail may encounter FTI. We submit 45-day notice regarding these employees. Is section 3 stating that because they’re government employees, we don’t need to include them in section 3.1?
    a. In the example provided above, the government employee should be considered a contractor. They should be included in section 3 of the SSR, and a 45-day notification should be submitted. Also, they should meet all the other contractor requirements. These individuals would fall under the internal inspections if the mail processing were at an agency facility.

18. **May we add state specific language to Exhibit 7 language requirements?**
    a. You may include small changes by the state in the Exhibit 7 language.

19. **How soon does the new Exhibit 7 need to replace the Exhibit 7 language in existing contracts?**
    a. You need to use the new Exhibit 7 language when the applicable agreements expire or are updated for any other reason. You don't need to amend existing agreements.

20. **Does the Corrective Action Plan (CAP) need to be in the Plan of Action & Milestones (POA&M)?**
    a. You need to track CAP items in a POA&M.

21. **Should we have only one POA&M that includes internal inspection findings as well as CAP findings?**
    a. No, there could be various POA&Ms that track different deficiencies. Also, you need to consider all deficiencies when performing security control and risk analysis.

22. **What does the two-barrier requirement look like at a telework site for paper federal tax information (FTI) (someone's home)?**
    a. Two barriers at a telework location for paper look like two barriers at the office. There should be two barriers between the employee who has a need to know and anyone else. An example is a locked box in a locked drawer.

23. **When will the new SSR template be available?**
    a. The template was sent to agency points of contact May 17, 2022. Agencies are expected to complete the new SSR templates with their current information.

24. **With the updates to the SSR template, are states expected to update the SSR in their 2022 submissions or 2023?**
    a. You can use the new SSR template for your 2022 submission, but it's not mandatory. It's mandatory for your 2023 calendar year submission.

25. **On the 2023 SSR, should we submit a new SSR with only answers for that year? Do we need the historical submissions on the SSR?**
    a. The SSR should only show the current operating environment. Historical data isn't necessary.

26. **Please explain how FTI may include personally identifiable information (PII). Do we assume that a file containing FTI and PII, is considered FTI?**
    a. Yes, personally identifiable information comingled with federal tax information will always be considered FTI. FTI may contain PII, but not all PII is FTI. If you're receiving PII from the IRS, it's always FTI.

27. **If an agency has a contractor that performed work on a modernization project that's completed, does the agency need to submit a 45-day notification or report it on next SSR?**

   a. If the contract is completed, a 45-day notification isn't necessary. Submit a 45-day notification before the contractor has access to FTI.

28. **You indicated there was a new template for the SSR. The IRS website indicates "The SSR is a living document. Do not start a new SSR using a blank template; use the accepted SSR template that was returned to your agency with the previous year's acceptance letter for submission." Should the state continue to use the SSR returned by the IRS after the last submission?**
    a. We've been adding this to the 2022 SSR responses in Section 1: "Please submit your 2023 SSR on the new SSR template updated for IRS Publication 1075 (Rev. 11-2021)." We provided the template to the primary agency POC. You can request it from the Safeguards mailbox: SafeguardReports@irs.gov. We're also working on updating the SSR site.

29. **If you have a policy that we do not print FTI, do we have to worry about this requirement on the printers? I understand no but wanted to confirm.**
    a. Correct. If there's a policy against printing FTI, the printers would not be in scope. If someone did print FTI, it would be considered a spillage.

30. **How should we correct a CAP finding that we believe was for another agency being reviewed at the same time? Do we make the Office of Safeguards know in advance or just indicate so on the next CAP due?**
    a. Open a technical inquiry (TI) to the Safeguards mailbox SafeguardReports@irs.gov to figure out the perceived issue and to address it. As we close out the TI, if the CAP finding should be closed, add a note to reference the TI.

31. **Are we required to inspect all alternate work sites?**
    a. Per Publication 1075, alternate work sites that are a residence no longer need inspection. If the alternate work site is a field office, it does need an inspection.