OFFICE HOUR CALL

Questions and Answers
September 2021

Subject: New Publication 1075: September 2021 Revision

Meetings:

Tuesday, September 28, 2021, at 1 p.m. ET (DOR) and 3 p.m. ET (FED/AG/SWA/DOT)

Thursday, September 30, 2021, at 1 p.m. ET (CS) and 3 p.m. ET (HS/ACA)

Tuesday, October 5, 2021, at 1 p.m. ET (Make-Up Call)

IT Q & A

1. **Is MFA required at the network level and at the application level to access the tax administration system?**
    a. Public facing systems granting access to Federal Tax Information (FTI) requires multifactor authentication (MFA). If the tax administration system at the application level is public facing, MFA is a requirement. If the tax administration system is a file server dedicated to providing FTI files and data storage over the network, MFA is a requirement. If MFA is initially required for network access, and an application is only accessible over the network, the network authentication can meet the MFA requirement even if additional (single factor) authentication is required for the application.

2. **Can you elaborate on the 14-digit requirement for system access?**
    a. Password length is a very important factor because the longer the password is, the harder it is to guess or break if compromised. For system access, Publication 1075 now requires that the user-generated password has a minimum of 14 characters.

3. **It said 14-character passwords on the slide, but Resource Access Control Facility (RACF) will only allow 8-character passwords. Would that be included in the requirement?**
    a. The requirements listed in Publication 1075 are technology agnostic, the requirements in IA-5: Authenticator management for password-based system requires passwords that are 14 characters long. The Safeguards Computer Security Evaluation matrices (SCSEMs) are our standard for securing and assessing systems that process, store and/or transmit FTI. If you are unable to meet the requirements within the SCEMs, a Plan of Action & Milestones (POA&M) will need to be developed where mitigations and compensating controls can be implemented.

4. **Concerning the password requirement, is the 14-character password for admin access or for all access? What is the password expiration range? Is there a one-day minimum to change your password?**
    a. 14 characters are required for all passwords. The expiration, character complexity, and lockout remain unchanged in the new Publication 1075.

5. **How about reuse of passwords? Is that still 24 generations?**
    a. Yes, it is still 24 generations.

6. **If a PIV card is used for access, does it change the PIN length?**
    a. The required password length, if a Personal Identity Verification (PIV) card is used for access, must be a minimum of eight characters.

7. **What if there are system limitations for password length and composition?**

a. If agencies cannot meet the composition requirements, then agencies need to adjust password length requirements accordingly. If agencies unable to meet both the password length and composition, then a POA&M for achieving compliance (e.g., upgrade/release the system) and risk mitigations needs to be established.

8. **The following language regarding new guidelines regarding verifiers and authenticators, which is not reflected in the current IRS Publication 1075: Verifiers SHOULD NOT impose other composition rules (for example, requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets. Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (for example, periodically). However, verifiers MUST force a change if there is evidence of compromise of the authenticator. Will the new Pub have NIST Special Publication (800-63) requirements for password/verifiers?**
    a. NIST, the National Institute of Standards Technology is the body that offers guidelines on technology and how to secure sensitive information. The Office of Safeguards has additional directives and requirements from the Internal Revenue Service and Treasury that we follow. The password (verifiers) requirements deviate from the NIST guidance.

9. **When will new SCSEMs and Nessus Files be coming out?**
    a. We are currently working on updating the SCSEMs as well as the Nessus files. Once approved, we will share the updated SCSEMs and Nessus files with all agencies.

10. **Secure MFD hard drives, can that be done with a seal?**
    a. No, a seal cannot secure Multifunctional Device (MFD) hard drives.

11. **SA-11 do you mean development environments?**
    a. System design helps in specifying hardware and system requirements and helps in defining overall system architecture. SA-11 now requires developer testing and evaluation at all post design stages of the system development life cycle.

12. **For the contractor that we hire to do the penetration test, does the contract need to have the exhibit 7 language and do we have to submit a 45-day notice for them? Also, since contractors are not allowed access to the FTI Benefits side, how would we do penetration testing for that side of the system?**
    a. Yes, exhibit 7 language is a requirement for any contractors who do any work for the FTI environment. Agencies that are authorized by statute to receive FTI and authorized to re-disclose FTI to contractors must notify the IRS at least 45 days prior to executing any agreement to disclose FTI to a contractor. If FTI will be disclosed to a contractor during a penetration test, a 45-day notification would be required.

13. **I would assume Exhibit 6 filings are still required for Penetration Testers.**
    a. All agencies intending to redisclose FTI to contractors must notify the IRS at least 45 days prior to the planned redisclosure.

14. **Regarding the IR-3 requirement for tabletop exercises, do the new requirements require all agency employees participate?**
    a. Tabletop exercises are only for those with an incident response role. However, agencies should coordinate with agency IT personnel, and when applicable, the data center as well as vendor personnel to protect the confidentiality of FTI.

15. **USGCB was mentioned. Can the IRS create SCAP files of the SCSEMs so they can be applied to devices?**
    a. All references to the United States Government Configuration Baseline (USGCB) have been removed in the new Publication 1075 and at this point there is no active plan for the Office of Safeguards to create Security Content Automation Protocol (SCAP) files of the SCSEMs.

16. **Are the cybersecurity requirements applicable to all state agencies (human services, child support, tax, etc.) or are there differences? We have a statewide IT office that oversees all agencies. If the requirements are all the same, it would be nice to be able to relay that to them all.**
    a. Generally, all the requirements are the same. However, access controls are going to be different since each type of FTI has different re-disclosure requirements under the IRC.

17. **In the case where the contactor is using state provided Virtual Desktop Infrastructure (VDI) that has MFA, which is locked down so no data can exfiltrate, would the remote (work from home) rule apply to the home office? What if it were a contractor alternative work site?**
    a. Agencies must maintain a policy for the security of alternative work sites. The agency must coordinate with the managing host system(s) and any networks and maintain documentation on the test. Before implementation, the agency must certify that the security controls are adequate for security needs. Additionally, the agency must develop and disseminate rules and procedures to ensure that employees do not leave computers unprotected at any time. These rules must address brief absences while employees are away from the computer

18. **Could you please clarify or provide examples of "exact location" level of detail needed on the FTI Log?**
    a. The exact location should provide enough information for an individual to locate the FTI media.

19. **Does the requirement for MFA for local users apply only for the user accessing any system that has FTI, or upon login into the domain?**
    a. The MFA requirement is for privileged and nonprivileged users (that can access FTI) whether it is local, remote or network.

20. **If a user can only access FTI after they have logged on to the network, is MFA needed for accessing the network and then again when logging into an application containing FTI?**
    a.
    If MFA is initially required for network access, and an application is only accessible over the network, the network authentication can meet the MFA requirement even if additional (single factor) authentication is required for the application.

Non-IT Q & A

21. **Would it be possible to get a copy of the PowerPoint for this presentation?**
    a. Yes, the IRS will send the presentation along with the questions and answers in approximately 2-3 weeks after this session and post them on the IRS.gov Safeguards Program Office Hour Calls page.

22. **Is there a way to sign up for email notice of future Office Hours Calls?**
    a. Due to limited spacing, we only send the invite to the IRS POCs and the IT POCs.

23. **Do you record these calls?**
    a. No, we do not record the WebEx.

24. **What time frame do we have to implement the additional requirements and changes to Pub 1075? What's the earliest Safeguards review date where the new 1075 will apply?**
    a. Six months after the publication.

25. **Is the published version of IRS Pub 1075 scheduled to be released in the first quarter of the 2022 calendar year or fiscal year?**
    a. It is scheduled to be released in the next couple of months, so the answer is fiscal year.

26. **There was a Pub. 1075 draft dated April 29, 2021. Should we assume that we should disregard that?**
    a. That version was sent to the agencies for feedback. Since that April date there have been more changes.

27. **Is it possible to get an updated draft prior to publication?**
    a. The final draft is near publishing so there will not be any more drafts to share. We are almost near completion on the final version.

28. **If disclosure awareness training is insufficient in the future, what is sufficient training in the future?**
    a. It is insufficient to only use the videos we provide for your Disclosure Awareness training. The video should be included as part of your Disclosure Awareness training program.

29. **Will the IRS provide updated training videos?**
    a. We will be looking into updating training videos. When updates have been made, we will provide that information.

30. **Are you going to provide us with disclosure training resources?**
    a. The resources are on the IRS.gov Safeguards Program Office Hour Calls website. Currently, there is no plan to add additional resources.

31. **Will you provide a crosswalk for all the section renumbering?**
    a. This is provided for you in the new Pub.

32. **Will Rap Back be sufficient for the reinvestigation requirements? Does Rap Back meet the 5-year requirement for background checks?**
    a. Yes, if you use Rap Back (continuous process) the requirement will only be the local law check.

33. **Regarding on-site reviews, moving forward could they be any one of the three types?**
    a. Hybrid review model will be used moving forward. You will be notified, in advance, of the type of review your agency will have.

34. **Are there any plans to fund the existing and new mandates? For example, reinvestigation from 10 to 5 years will be an added expense and all the cyber security updates appear to be more expensive to the agencies.**
    a. There are no plans to fund the existing and new mandates.

35. **On prior IRS reviews, blurring of TOPS offset payments was allowed with 3 other payment method sources. Three years ago, it was changed to 5 payment sources. On our review this year it was stated that blurring is no longer acceptable, and IRS is waiting on legal interpretations. Has anything changed or any new guidance on this topic?**
    a. Currently, there have been no changes. Blurring is no longer acceptable. We have no new guidance on this topic.

36. **Will there be updates to the Telework section of the 1075, specifically will IRS place more standards on the agency in that section?**
    a. There are some updates to the Telework section of the 1075. You will be able to see those changes within the highlighted section.

37. **Can you provide an example of an inventory of key logs? Can we get a copy of that example of an inventory of key logs?**
    a. The logs which were shown during the presentation were FTI logs and are in Publication 1075. The key logs differ from agency to agency and are not as defined as an FTI log. Key logs can include who has the key, when it was given to them, the number of the key, when it was returned, etc.

38. **I am looking at Pub 1075 (2016) and counted 20 policy topics but only 13 on the PowerPoint. Were some of these combined or deleted in the new version?**
    a. The policies have expanded on the NIST security control families with the expansion of the control catalog.

39. **Will the Office of Safeguards be providing a template for the annual certification of contractors?**
    a. Yes. We will be providing a template for the annual certification of contractors.

40. **Any changes to the contractor language?**
    a. Ensure you've submitted your contractors on our 45-day notifications.

41. **Will the PSE call still occur 60 days prior to the on-site visit?**
    a. Yes, that is our objective. The hybrid review will start two weeks prior to the onsite visit.

42. **To be clear, are policies updated every 3 years and procedures annually?**
    a. We've changed the requirement to updates and re-writes to every 3 years for policies AND procedures.

43. **Can we have a copy of the 86 revisions, or must we wait?**
    a. You will have to wait for the publication.

44. **Could you please clarify or provide examples of the "who has access" level of detail needed on the FTI log?**

a. This would be a column in the FTI log of who has access to the FTI (for example, receptionist or a name)

45. If a high-volume printer is in a locked room, will that meet the MPS, or do we still have to physically lock the hard drives?

a. Ensure the printer has a minimum of two barriers. It must either meet Minimum Protection Standards (MPS) and the requirements for MPS (for example, FTI is behind two barriers), or you need to have a locking mechanism for the multifunction device with a hard drive.

46. Does a video camera or other surveillance count as one barrier for MPS?

a. No.