OFFICE HOURS CALLS

Questions and Answers
December 2021

Subject: Taxpayer First Act (TFA) Section 2004

Meetings:

Tuesday, December 14, 2021, at 1 p.m. ET (DOR) and 3 p.m. ET (FED/AG/SWA/DOT)

Thursday, December 16, 2021, at 1 p.m. ET (CS) and 3 p.m. ET (HS/ACA)

IT Q & A

1. **Will the new Safeguard Security Report (SSR) template include guidance for specific controls?**
    a. We're adding more guidance in the SSR to make it clear what information you should include for each control.

2. **If the cloud vendor is Federal Risk and Authorization Management Program (FedRamp) certified, will that exempt them from these requirements?**
    a. FedRamp authorized Cloud Service Providers (CSPs) don't need on-site inspections due to FedRamp continuous monitoring and assessment requirements.

3. **How does Taxpayer First Act Section 2004 (TFA 2004) affect National Association of Information Destruction (NAID) certified contractors? The 2021 Publication 1075 exempts NAID certified contractors from the 18-month internal inspection. Under TFA 2004, are we back to conducting internal inspections?**
    a. Currently, agencies don't need to conduct on-site reviews on NAID certified contractors.

4. **If a contractor is remote (only accesses via Virtual Private Network (VPN) to a server on our site or a virtual desktop) but NEVER saves any data to their machines on their site, and the data resides on our servers here, do we need to do an on-site review of their site?**
    a. You need to make sure your information system is configured, so they can't save any data on their machines at their site (see VDI SCSEM). The contractor is still subject to a physical security on-site review to ensure users are receiving training, background checks, etc. and that the facility has MPS in place.

5. **When state agencies conduct internal reviews, we issue Plan of Action & Milestones (POA&Ms) and monitor resolution. Will we do the same with the on-site reviews we conduct under the TFA?**
    a. Yes, you'll do the same for the on-site reviews.

6. **In reference to vendors working from residential worksites, will we be required to perform on-site inspections?**
    a. No. We don't require inspections or reviews of residential locations. The agency must have telework requirements in place with the vendor that meet requirements in Publication 1075, Section 2.B.7.

7. **Our equipment has federal tax information (FTI). Would data centers that house our state-owned equipment need these on-site reviews even though they don't have access to any of our FTI? They only "house" our equipment, which has FTI?**
    a. Yes, you need to review the data center. It's a contracted location that requires an on-site review per Taxpayer First Act (TFA) Section 2004.

8. **We have a contracted data center. They don't have access to FTI because the data store there is encrypted, and they don't have access to the encryption key. Do we need to include this location in an on-site contractor review?**
    a. Yes, because you still need to conduct physical security checks.

9. **Are other state agencies that maintain our IT infrastructure (i.e., network, firewall, hardware etc.) considered contractors? For example: Family Services' (primary state agency that handles FTI) IT equipment managed by Enterprise Technology Services (another state agency).**
    a. State agencies aren't considered contractors. A state agency would have an SLA and an internal inspection.

10. **Can we use the Safeguard email Public Key Infrastructure (PKI) to encrypt submittals?**
    a. No. Per Publication 1075, we ask agencies to encrypt the files using Secure Zip or Secure Data Transfer (SDT).

11. **South Dakota has a consolidated IT infrastructure with a contracted data center in Boulder, CO. I do all state audits. Can I complete the worksheet once for all my agencies that use FTI?**
    a. Yes, agencies may share on-site assessment results the same as internal inspections if location, contract terms and implementation are similar.

12. **Regarding VMware, we're not using ESXi to store information; we're only using it for a host. Do we need to follow both the SAN SCSEM and VMware SCSEM? The VMWare Safeguard Computer Security Evaluation Matrix (SCSEMs) are outdated. When will you update that?**
    a. If an agency is processing or transmitting FTI via ESXi, then the ESXi SCSEM applies. If the SAN is storing FTI, then that SCSEM applies. Both SCSEMs may apply. We'll update the VMware ESXi SCSEM by the end of March 2022.

13. **Will IRS Safeguards update the SSR to mirror the new Publication 1075 naming convention? For example, the older version of Pub 1075 has Section 9, Information Security Controls, and the new 1075 has Section 4, NIST 800-53 Security and Privacy Controls.**
    a. The draft SSR template doesn't mirror sections in Pub 1075 (11-2021). NIST controls in Pub 1075 (11-2021) are under Section 4. They're Section 6 in the draft SSR template (subject to change). It will have all controls, enhancements, and requirements from Publication 1075 (11-2021) along with TFA 2004 requirements.

14. **What's the process if an agency identifies a contractor deficiency and cannot certify compliance? I understand we'd need a corrective action, but are you saying we'd need to take all corrective actions before SSR certification is due?**
    a. This is where risk management (e.g., POA&MS) and working with your contractor to mitigate risk (e.g., compensating controls) applies. If there are findings, we request the agency make a risk based decision as part of the certification process.

15. **What if the contracted data center is run by an agency in another state? For example: State A contracts with state B to use their data center for disaster recovery (DR) and backup?**
    a. Since the data center is contracted, you'll need to review it. This would be a great time to have a DR test exercise.

16. **Wyoming has a Service Level Agreement (SLA) with the Wyoming Department of Enterprise Technology services (ETS). ETS is the holder of the contract with the contracted data center that all FTI passes through. How would this be addressed for an on-site review of the contracted data center and the review of the data center where the data backups are stored?**
    a. Wyoming agencies must conduct an on-site review of the contracted data center and any contracted disaster recovery sites.

Non-IT Q & A

17. **Do we need to duplicate information already provided on the new worksheet?**
    a. Yes. We're building the database with information submitted for the contractors. But, based on when that data was requested, it may not the most current information. Now, we're looking for the most current information. If you provided some of the information before, you'll have to put that on the new worksheet and anything that's changed will need updating.

18. **For certification of the contractor, do we only need to certify contractors receiving FTI at their site (not contractors on our sites) on the worksheet?**
    a. You need to review all contractors with access to FTI. Some of the questions won't apply; some items will apply. You'll need to fill out the form accordingly.

19. **Are remote reviews acceptable if the contractor is in another state and their workers are teleworking?**
    a. You're not required to do on-site reviews at residential telework sites. If the contractor uses a common office space and only teleworks occasionally, you'll need to review the office space.

20. **Will we need to update the previously submitted contractor worksheets before 1/1/2023?**
    a. Although you completed worksheets previously, you'll need to also complete the new worksheet that IRS Safeguards will send to agencies next year (2022). You'll need to complete that current contractor worksheet and submit it with your annual SSR beginning in 2023.

21. **When do we need to implement use of the on-site review template? Before or after 1/1/2023?**
    a. After January 1, 2023, because the requirement doesn't start until then.

22. **For clarification, is the requirement that we must perform an on-site review if a contractor receives FTI only? What if a contractor is a third-party vendor that could have access to view FTI, if we grant them access?**
    a. If they may have access to or receive FTI, then you'll need to conduct an on-site review for that vendor or contractor.

23. **I missed the date. What is the effective date of the new Publication 1075?**
    a. June 10, 2022

24. **For clarification, effective January 1, 2023, Section 2004 of the Taxpayer First Act (TFA) requires that no FTI shall be disclosed to agents of agencies unless the agency conducts reviews and certifies that their contractors provide appropriate safeguards. Is this correct?**
    a. Yes, the agency on-site review schedule for contracts in place after January 1, 2023 must be followed.

25. **If a contract is one month long, do we have to do the review after two weeks into the contract?**
    a. Contracts six months or less will not require an on-site review.

26. **How are contracts handled if there's not a set time frame or end date? When would we need to do the on-site review (e.g., for an annual financial audit)?**
    a. We consider contracts with no end dates to be more than three years, and you would need to do an on-site at the three-year mark.

27. **We have a state-run data center, so I understand that we must review them every 18 months. If our backup site is operated by a different out-of-state data center, do we have to review them every three years then?**
    a. If your backup site is operated by a contractor, then the contract and the duration of the contract will determine when you'll conduct the on-site review. If it's an ongoing contract, you'll need to conduct the review every three years.

28. **Are these on-site reviews different than the internal inspection an agency already must do annually?**
    a. Yes, they're different than internal inspections. The on-site review replaces the internal inspections for contractors.

29. **Does this apply to Health and Human Services (HHS) agencies, which cannot allow contractor access to FTI? Our contractors aren't allowed access to FTI due to federal statute.**
    a. If you don't have contractors, this shouldn't change anything for you. You'll just need to state that on your SSR once we update the SSR for TFA 2004. If they don't have access to FTI (including admin access on IT that could facilitate access/bypass access controls), then it doesn't apply. The contractors aren't within scope for Safeguards.

30. **Under current law, HHS type agencies cannot permit contractors to access FTI; only agency employees can do so. Other agency types like child care and revenue could permit contractor**

access to FTI. Did Section 2004 change the law to allow HHS type agencies to permit contractors access to FTI?

a. TFA 2004 didn't change the law to allow additional disclosures to contractors. The statement about contractor on-site review under TFA 2004 is for all agencies that may using contractors regardless of agency type.

31. **Do we need to have an independent auditor perform this contractor assessment? Or can the agency security lead conduct it on their contractors?**
    a. You don't have to have a special internal or external auditor. An agency employee can conduct the on-site review.

32. **Are we submitting proof of "pass" documentation with this report such as screenshots showing logs or other things?**
    a. Currently, agencies don't have to submit evidence. We may request it in the future.

33. **On-site reviews take place every three years with certification provided annually, is that correct?**
    a. Yes, if the contract is more than three years. If the contract is less than three years, then the review would be at the midpoint of the contract span.

34. **Will a link to the templates (e.g., internal inspection report) be sent out to each of the states, or will they be available on IRS.gov?**
    a. Once we've finalized the on-site review template and the contractor review worksheet, we'll put them on the Safeguards section on IRS.gov. Also, we'll send the templates with your SSR, and you can send an inquiry using the IRS Safeguards email address.

35. **Can you guys elaborate on ATO certs? I want to know if those are acceptable for proofs of audit**.
    a. No. You must complete the on-site review template.

36. **When will the new SSR be available for us to review? Also, can we look at a draft copy if you're making a lot of changes to it?**
    a. Tentatively, April 2022. Currently, a draft copy isn't available.

37. **Will you update the Internal Inspection Report templates too?**
    a. The updates for internal inspections won't include contractors.

38. **Our next audit is June 10, 2022. Which version of the Publication 1075 will we be audited against?**
    a. The review will leverage the 2016 version.

39. **States will have limited resources also. What is the distinction between an on-site inspection and an on-site review?**
    a. There's not an on-site inspection; There's an internal inspection and an on-site review. TFA 2004 requires on-site review of contractors effective January 1, 2023. Internal inspections are the same, but for contractors you'll conduct an on-site review.

40. **Contracts may be a set time with x number of one-year extensions. Are you looking for the farthest date out or the date of the baseline contract?**
    a. If the original contract is less than three years, you need to conduct the on-site review at midpoint of the contract. After the original contract ends and the extension or option years begin, you need to conduct on-site reviews every three years.

41. **Does this mean the IRS will not visit contractor sites during Safeguards audits? If so, are you asking us to do the equivalent of an audit with our contractors?**
    a. No, it doesn't mean disclosure enforcement specialists won't come out and perform the on-site reviews of the contractors. Safeguards always reserves the right to do a review on contractors and conduct a full Safeguards review.

42. **Will a separate worksheet be used for each contractor, or will all contractors be listed on one worksheet?**
    a. All contractors will be listed on one worksheet.

43. **We're only submitting contractor and subcontractor on-site reviews the year each one is due and with that year's SSR?**
    a. Yes, the on-site reviews completed will be reported on the SSR that covers that annual reporting period.

44. **We currently use the old version of the internal inspections report for our internal inspections. Do we need to change to the newer version posted on the Safeguards website, or can we continue to use the old version?**
    a. We would like for agencies to use the latest version of the internal inspections report. We'll post the updated internal inspections forms and the new TFA on-site review template to the Safeguards section on IRS.gov.

45. **For a state-run child support program that contracts with several county DA offices to provide full Title IV-D services in those counties, are these reviews required for those offices?**
    a. County offices with government employees will require internal inspections but not the TFA on-site review.

46. **Wyoming has contracts with the clerks of courts in the counties, so would they be considered county employees or contractors?**
    a. County government employees do not fall under TFA 2004.

47. **What about contracted staff who are not county staff, such as IT staff who work along with state staff? Do we treat them like county staff?**
    a. Contracted IT staff fall under TFA requirements for contractors.

48. **Starting in Jan 2023, we'll no longer have to do an internal inspection of our contractors. Are you saying we'll switch to doing TFA on-site reviews of our contractors starting Jan 2023 instead? Is this correct?**
    a. Yes

49. **Are individuals hired under a contractor, who supplies candidates to the state, all required to do on-site reviews? These are individuals who work at the state office. The contractor who supplies the candidates doesn't have FTI access.**
    a. You need to review all contractors with access to FTI. Some of the questions won't apply; some items will apply. You'll need to fill out the form accordingly.

50. **If the IRS has completed the review during the year our TFA review is due, do we still complete the review for that year?**
    a. If the contractor's on-site review is within 3 months before or after the month of your Safeguards review, you don't need to conduct a TFA review,

51. **If an on-site review is conducted at the beginning of a contract, would the agency have to still do a midpoint review as well. For example, a one-year contract begins January 1, 2023, and the agency does on-site review January 15, 2023. Are further reviews needed?**
    a. No. You don't need to do other reviews because you can do on-site reviews early.

52. **Is it possible to get confirmation in writing that our scheduled audit of June 10, 2022, will be against the 2016 version of Pub 1075, please?**
    a. The 2016 version of Publication 1075 applies to all reviews that start before release of the new version of the publication.

53. **If the contractor is based out of state, does the agency have to physically go on-site to examine the contractor's site to obtain the evidence?**
    a. Yes

54. **Will you send us the template you want us to complete for the contractors moving forward?**
    a. Yes.

55. **Regarding the on-site visit with contractors, our policy states that contractors aren't allowed to work with or access any FTI from their business location, only from the Census Bureau HQ facility or at home (due to COVID). Does that affect the on-site review process?**
    a. On-site TFA reviews don't apply to contractors working from home. Telework policies apply.

56. **Will there be a new SSR template developed to follow the new Publication 1075 format?**
    a. Yes, and it will include TFA 2004 requirements as well.