OFFICE HOURS CALLS

Questions and Answers
November 2022

Subject: Implementation of Taxpayer First Act (TFA) Section 2004

Meetings:

Tuesday, November 1, 2022, at 1 p.m. ET (ACA/FFM/HS/SBM) and 3 p.m. ET (AG/DOT/FED/SWA)

Thursday, November 3, 2022, at 1 p.m. ET (DOR) and 3 p.m. ET (CS)

IT Q & A

1. **For cloud services that are Federal Risk and Authorization Management Program (FedRAMP) authorized, are we expected to conduct on-site inspections? Ex. AWS, Microsoft**
    a. You won't be required to conduct on-site reviews for FedRAMP cloud service providers since FedRAMP has a continuous monitoring and annual assessment requirement.

2. **Since "protect" was added to Publication 1075, do we have to do 45 Day letter for "systems" we use to protect FTI, even systems we procure for our cloud environment?**
    a. If FTI is being stored or processed in the cloud, you need a 45-day notification. If it's not actively processing or storing FTI, you don't need a notification. Please submit the question with more specifics to the Safeguards mailbox: **safeguardreports@irs.gov.**

3. **We currently use Secure File Transfer Protocol (SFTP)/tumbleweed server to send our documents (CAP, SSR, etc.) to IRS. I'm guessing that we will be allowed to submit this document, as well, as we don't send such documents across email.**
    a. Yes, the agency can continue to submit documents through SFTP/tumbleweed server.

4. **FedRAMP contractors do have to be noted on the contractor worksheet, even though they are not subject to on-site inspection, correct?**
    a. FedRAMP contractors still need to be listed on the contractor worksheet, with a comment in the comment section that a review won't be conducted and why.

Non-IT Q & A

1. **Clerk of Courts is our contractor. There are a lot of IT questions in the questionnaire to which none of those entities would have any knowledge on, since they refer to the state. How do we handle those questions?**
    a. Mark as N/A and add a justification or a comment to briefly explain that the contractor uses state IT and therefore it's not applicable.

2. **Does the TFA apply to a finding regarding contractors from 2022, or are we still subject to the internal inspections and the TFA now when we submit the Corrective Action Plan (CAP) in February 2023?**
    a. If the agency intended on conducting the internal inspections to correct a finding, they should use the on-site review template in place of the internal inspection template. This would meet the requirement of the finding and an on-site review would be conducted early.

3. **If the contractor has fails, the instructions state that the contractor must complete a plan of action and milestones (POA&M) document. Will the IRS require agencies to submit a copy of POA&Ms with the SSR?**
    a. No. In the instructions it does say that the agency needs complete a POA&M. The agency will keep the POA&Ms on-site, and Safeguards will review the POA&Ms when it does its Safeguards review (three years). Agencies don't need to submit these POA&Ms to the IRS, only the on-site checklists and contractor worksheet.

4. **Is a consolidated data center deemed to be a contractor?**
    a. A state-run data center isn't deemed a contractor for TFA 2004 requirements, but a data center run by a contractor is a contractor. The internal inspections will still apply to a state-run data center. However, if it's run by a contractor, then the on-site review will need to be completed.

5. **Will these reviews take the place of internal inspections we already do every 18 months on our shredding contract and our storage contractor facilities?**
    a. Yes. The on-site reviews are taking the place of internal inspections for contractors.

6. **Since the state data center is another state agency (not a signing authority of FTI), then are they considered a contractor?**
    a. If the data center is another state agency, the internal inspections will be conducted for that location.

7. **Since the worksheet must be submitted annually, but we are required to conduct the review once every three years (for a three-year contract), do we just resubmit the same form two out of the three years?**
    a. Yes. Re-submit.

8. **Will the on-site need to be done for those contractors that have logical access to FTI, but FTI is not stored physically at rest at the contractor's site, i.e., data center?**
    a. Yes. The agency will still need to do an on-site review.

9. **How does the naming convention work for agencies that have multiple types (i.e., CS, HS, ACA)?**
    a. The naming convention will include each type (i.e., CS-HS-ACA).

10. **Are agencies allowed to hire third-party assessors to complete the annual review of contractors as long as the agency creates a POA&M from the review and works to resolve any findings?**
    a. Safeguards is going to allow third-party assessors to complete the annual review. The guidance for this is being worked on, but the agency would still be responsible for the POA&M and remediation of the findings. There will be certain restrictions to the third-party assessor and that will come with the guidance.

11. **We perform annual reviews of our contractors, we have a review schedule for December 2022, and our SSR is due 2023. We will submit the contractor worksheet, but will it be accepted if we submit the current internal inspection template?**
    a. Yes. The actual contractor worksheets aren't required until after January 1, 2023. The agency is completing the internal inspections in December, which will be submitted with the SSR due in 2023. Based on the duration of the contracts, starting on January 1, 2023, is when the agency should make the next determination of when the on-site review is to be conducted.

12. **If a State Data center ran by the state is not considered a contractor, do we still have to have a service level agreement (SLA) with them?**
    a. Yes. An SLA is needed. Ensure that it has all the required language in it from the 1075, effective June 10, 2022.

13. **If we are doing an internal inspection later this month, should or can we use the new template?**
    a. You can use the new template; it would be called the on-site review template. Safeguards is trying to differentiate between the internal inspections and the contractor on-site reviews.

14. **Can the contractor self-certify by filling out the document and the agency completing a phone or Teams interview?**
    a. No. The on-site review needs to be conducted in person.

15. **If "embedded" contractors are working from the same location on the same system as W-2 employee staff, do we need to complete both our regular on-site inspection reports and the on-site inspection report specific to contractors?**
    a. No. The internal inspections would be conducted for the location those "embedded" contractors are working.

16. **Should we leverage third-party assessment for the TFA?**
    a. Safeguards will allow third parties to do assessments for TFA. There are several examples and guidance being worked on right now to be sent out regarding the use of third-party assessors.

17. **With the statement that there will be a corrective action, does that still mean it is a failure, even if they could show that they would rectify the issue within, say, 48 to 72 hours?**
    a. Yes. It's still a failure. You would be listing the failure in the POA&M and showing that it was remediated within 48 or 72 hours.

18. **Do you tell them on the spot that they failed?**
    a. Yes. Tell them if they weren't aware, or if the reviewer was relying on evidence, tell them it would be marked as a failure if they don't provide it.

19. **How strict is the mid-point requirement for contracts less than three years? If we have a bunch of contracts that are on the same contract period, and their mid-points would all be the same, can we spread them out plus or minus six months?**
    a. Safeguards doesn't want the reviews to be done late. The agency can certainly do the reviews earlier.

20. **Can you please address self-assessments?**
    a. There are no self-assessments in on-site reviews for contractors.

21. **Will contractors that are National Association of Information Destruction (NAID) certified still be required to be identified on the contractor worksheet review, but not the review template with the questions? The NAID-certified contractors will not be required to complete a Safeguard review. Is this correct?**
    a. You still need to put them on the contractor worksheet, but in the comment section, you can identify that it's NAID certified, and no review required. Safeguards will still need to know they're contractors of the agency.

22. **When is the first TFA review due and what's the frequency of the review?**
    a. It depends on the duration of the contract. If it's less than three years, it's done at the mid-point of the contract. If it's longer than three years, it's every three years. For calculation purposes, please begin on January 1, 2023.

23. **Do we need to use the template or something in similar form?**
    a. Yes. You need to use the exact template we're providing because those answers serve as findings.

24. **Do we need to answer all the questions on the TFA worksheet? Is it acceptable to send out the TFA questionnaire for the contractor to complete?**

a. These are on-site review questions. No template should be sent. The agency needs to take the on-site review template and be face-to-face with the contractor for completion.

25. **Just want to clarify, these are in-person, face-to-face interviews to have with each contractor with access to FTI, and this cannot be held virtually, correct?**
    a. Correct, the statute says on-site.

26. **Does a significant event change the assessment cycle for the contractor?**
    a. It doesn't change the assessment cycle for the contractor, but outside of the TFA requirements if there is a significant change in the environment, the agency should conduct an assessment if risk is increased.

27. **Is TFA only applied to contractors who have direct access to FTI data? What about administrators who are contractors? Are they in scope?**
    a. It applies to all that have access or the ability to access FTI, administrators included.

28. **Is the voluntary use of the IRS on-site inspection report, made available by Safeguards, now mandatory?**
    a. Safeguards has provided and will provide again after this office hour call a NEW on-site review template and a NEW contractor worksheet. These new templates are required for TFA compliance. The Internal inspection templates you're referencing will still be available for the locations where you'll be conducting internal inspections (headquarters, data centers and field offices).

29. **Minnesota contract process is to execute agreements for two years with annual extensions for up to three years, making the contract a five-year agreement. For inspection planning, should we be using five years or two, then three, then four and then five.**
    a. You should be using the first two years of the contract for planning purposes for the review. When the extension begins, you'll need to plan a review for the duration of the extension.

30. **Would an on-site shredding company that does not directly access, receive, or review paper FTI be considered a contractor in this regard?**
    a. Yes. The on-site shredding company would be a contractor, but the on-site review wouldn't be required for this contractor. You'd need to make mention in the comment section of the contractor worksheet that an on-site review of this contractor won't be conducted.

31. **We have a number of contractors and a majority of them work within our secure environment and infrastructure, in our facility or telework same as any other agency employee. FTI doesn't leave our environment and is not processed or stored anywhere**

else, so there is no facility to review. Do we note this in the "comments" section of the worksheet as to why a review is not performed?

a. Still capture it in the internal inspection. List them on the contractor worksheet but explain why a review isn't being done.

32. **We have a vendor that provides a space in the data center, all the equipment we manage and have control over. Looking at the contractor inspection we would do the physical inspection portion, but they don't have any control over the inner workings of the computer systems. Do we just complete the first half of the physical inspection?**
    a. Correct. If you're putting down N/A, please leave a comment and say that contractors don't control IT or store FTI on IT, all IT is agency run.

33. **If a contractor location is within another state, are virtual meetings to complete the review ever acceptable? Are we supposed to fly halfway across the country to do these on-site reviews? Can we coordinate with the state where the contractor is located?**
    a. No. Virtual meetings aren't acceptable for the on-site reviews. Remember that you should have already been conducting internal inspections on-site prior to the implementation of TFA. You can coordinate with an agency in the same state as the contractor to conduct the on-site reviews.

34. **On the contractor worksheet for the agency POC name, should this be the person that is the POC for the contractors?**
    a. The name of the point of contact should be the POC from the agency, not the contractor. You could include both, but make sure they're identified appropriately.

35. **Data Centers and all their subcontractors will NOT undergo a TFA 2004 onsite review, but we will continue to do the IRS internal inspection of our data center and all associated subcontractors working out of the data center. Is this correct?**
    a. If the data center is a contracted site, it should be treated like a contractor and undergo the TFA review. If it's a state-owned data center, it will fall under the internal inspections and not the TFA onsite review.

36. **What is the definition of "disclosing" regarding contractors? IT personnel may have logical access to the network, but I am not "disclosing" FTI to that contractor. Does "disclosure" include physical and/or logical access to hardware and data?**
    a. If they can access data, no two barriers between them and the data or if they're administrators and can change permission to access FTI, then that's access. If they are truly segregated on the computer systems, they might not have access depending on the setup. Access to or the ability to access all counts as FTI being disclosed to the individual.

37. **Child support agencies are not experts in all the areas of IT you include in the on-site reviews. How do you propose/suggest these on-site reviews are conducted appropriately?**

a. There are third parties available (i.e., auditing firms). Maybe leverage from state information technology to help bring you up to speed or come along with you.

38. **Please confirm if contractors that have a service or supplemental staff agreement to conduct child support work at county field offices such as friend of the court and prosecuting attorney offices with contracted staff will not be part of the TFA2004 review, but they will still be subject to internal inspections.**
    a. You're correct about the service or supplemental staff agreements to conduct CS work at county offices would be included in your internal inspections and a separate on-site review would not be necessary.

39. **If the contractor submits a third-party audit report, will that be acceptable?**
    a. The third party should be arranged/contracted by the agency, not the contractor being audited/reviewed.

40. **Will the new templates for the on-site reviews and internal inspections include a script along with it? The templates seen so far have a review question per line, but there are several follow-up questions that are not on the template. For example, in the second role play, the first question was about how access is granted, but they went further to ask for a copy of the policy. It didn't state on the template that we needed to get copies of that policy. (Then, out of curiosity, would that policy need to be provided with the final document to the Office of Safeguards?)**
    a. There is no script necessarily. Safeguards provided the questions in the template. It depends on some of the answers given during the review. Don't be scared to delve further into the topic to get the answers which will lead to the pass/fail decision.

41. **We have a contractor on a 10-year contract. On January 1, 2023, there will be two years remaining on the contract. When would an on-site review be required? Is the three years based on the remaining time left on the contract as of January 1, 2023, or from the start of the contract?**
    a. Even though the contract is 10 years, on January 1, 2023, there would only be two years left. That means since it's less than three years so the on-site review would need to be done at midpoint, which would be a year.

42. **Many of our contractors work at our headquarters site. How are these reviews handled?**
    a. Your contractors would fall under your internal inspections conducted for your headquarter location.

43. **What about a data center that is owned by a corporation, but the state has a secured suite within that data center? Everything on the suite is owned by the state.**
    a. There are still portions of the checklist that would need to be conducted. You can mark things as N/A and leave a comment about why. For instance, the data center may need to have an incident reporting procedure. If someone breaks

into the building, do they need to report it to you? Do they provide any of your two barriers? These are checks in A-G, and you would likely mark H N/A since they're not managing an information system.

44. **Is this still a correct statement: contracts with less than 11 months remaining on the contract as of January 1, 2023, are not subject to review?**
    a. Yes.

45. **Will we need to send a control file with the zip file?**
    a. You won't need to send a control file. Please keep your control file accessible for the Safeguards personnel that will be on-site during the three-year safeguard review.

46. **We are turning in our SSR this month and planning on turning in the new SSR 2.0. Is this correct, or should we still be using 1.2?**
    a. You can use either template. The 2023 submission will need to be on the 2.0 template.

47. **We conducted all our 18-month internal inspections from August-October 2022. Will those internal inspections be accepted with our March 2023 SSR?**
    a. Yes. They'll be accepted because they were done back in December and requirements of TFA don't start until January 1, 2023.

48. **Just to clarify: when submitting the SSR, we must also submit the contractor worksheet or review template?**
    a. Yes, you must submit the contractor worksheet and templates with your SSR.

49. **Our SSR is due February 28, 2023, and I know that the TFA documents are required to be submitted with it. If we switch to Amazon Web Services (AWS) for our servers and systems that store FTI in first or second quarter of 2023, will we still be required to submit the TFA documents with the SSR for AWS? Also, will we still be required to do an on-site review for contractors who stored FTI for those months that we were NOT in AWS? Lastly, if we used the old method of self-certifying IIRs back in May 2021, will that be a sufficient sample to include in our SSR due February 28, 2023?**
    a. Table 4 in Publication 1075 (SSR Submission Dates) provides guidance for the reporting period that each SSR submission should cover: February 1, 2022-January 31, 2023, for a February 28, 2023, submission. You will need to submit a 45-day cloud notification prior to migrating to AWS and AWS should be listed on your contractor worksheet submitted with your 2023 SSR. If the contractors didn't have FTI for at least five months into 2023, you're not expected to do the TFA 2004 on-site assessment. The internal inspection templates are sufficient for 2022.

50. **For some contractors, the number of workers varies during the reporting period (Column J, # of contractors). What number do we provide in our report, the number at the end, start or average of the SSR reporting period?**
    a. The agency should use the number of contractors at the start of the contract. In the comment section, please indicate that the number of contracts could vary through the duration of the contract.

51. **What if a contract went for five months into 2023 and your SSR is due before that? Would we have to do a review at 2.5 months? Is there a minimum, being that if we have a contractor for only a month, are we required to do an on-site review at 15 days?**
    a. No. A review isn't necessary. There is a five-month minimum.

52. **The difference between our centralized IT (which is a different agency) and in the terms of Publication 1075, they are considered a contractor. However, in the terms of the IRS they are not since another agency is not considered a contractor. Can you clarify this?**
    a. For TFA 2004 government employees of the same state aren't considered contractors. However, for disclosure, they're not considered part of the agency, so other statutory disclosure restrictions may apply.

53. **Do we need to retain the POA&M on-site for five years?**
    a. Yes.