Office Hours – September 2018

Topic: Cloud Computing with Federal Tax Information (FTI)

1. **When a state-managed solution is offered to all agencies, is this considered a cloud solution? Would any encryption keys need to be retained and managed by the agency in this instance?** If the state IT function (state employees are managing the cloud solution) manages the solution, the agency doesn't need to keep and manage the encryption keys. But, anyone who hasn't received training, doesn't have a need to know, and has no legal authorization for redisclosure shouldn't access FTI. For specific questions, please send an email to safeguardreports@irs.gov.

2. **What level is acceptable for data encryption at rest?** Agencies need to protect data so the cloud vendor cannot get access to it. Agencies should encrypt data so the cloud cannot access the encryption in storage. All encryption must meet FIPS 140-2 requirements.

3. **Can you discuss any unique security related to on-premise cloud solutions where there is a shared responsibility from an external agency, but the solution is on-premise?** This isn't considered a cloud that needs to be reported as a cloud environment. Safeguards wouldn't enforce cloud requirements on this solution. Safeguards would assess this with traditional SCSEMs (Virtualization SCSEM). For security, agencies should lock down access to any "need-to-know" areas. If the IT function doesn't need to have access, agencies should have logical access controls in place.

4. **When using a vendor-managed solution using FedRAMP certified PaaS (AWS PaaS), would the vendor-managed solution require separate FedRAMP certification as well for SaaS?** FedRAMP is largely solution based. It depends on if a vendor manages solutions in the same data center with the same controls or if they're logically separate products. Safeguards would like to see FedRAMP authorization for every service model contracted by the agency. For specific questions, please send an email to safeguardreports@irs.gov.

5. **What should an agency do if their cloud vendor is not FedRAMP certified?** Between now and the on-site review, the vendor can go through the FedRAMP authorization process. If Safeguards conducts an on-site visit and finds FTI on a non-FedRAMP authorized cloud, this would result in a critical finding. The agency would have to remove FTI from the cloud and certify removal. If the vendor is working toward FedRAMP authorization, the agency should note this during the CAP process, and Safeguards will take this into consideration. Unless the vendor achieves FedRAMP authorization and certifies it, the agency may not use this service. In this situation, the agency will need to show proof that it deleted records associated with that cloud service.

6. **Where are the cloud requirements published so agencies may share this information with vendors?** Link to technical memo: https://www.irs.gov/privacy-disclosure/cloud-computing-environment

7. **Can you talk about multifactor authentication (MFA) expectations with the cloud?** If your cloud vendor solution doesn't have a dedicated route between the agency and the cloud solution and all credentials are in the cloud, Safeguards would like to see remote access multifactor authentication carried out—this would be true remote access. MFA isn't needed for every login using a mobile device, such as checking email using O365, but agencies must carry out a Mobile Device Management (MDM) or Mobile Application Management (MAM) solution. This means the agency either manages the device completely or remotely wipes all data from the device, plus control the authentication process.

8. **Should the contractor notifications be sent in via the notification form? Safeguards** will process a notification sent as a letter but strongly encourages agencies to use the contractor form for prompt processing of their requests.

9. **Is there a plan to expand the number of cloud vendors IRS will be working with in the future for SCSEM development?** Safeguards hopes to work with other vendors if it makes sense. Agencies may procure cloud services from any vendor that's onshore, FedRAMP certified and meets the other requirements listed in the cloud computing technical memo.

10. **Can you revisit the requirements to visit a site of a cloud location vs. a location which is considered hosted (where a mainframe may be located)?** With FedRAMP authorized clouds, Safeguards doesn't do a site visit. The Disclosure Enforcement Specialist (DES) will do an on-site review of hosted centers to make sure physical securities are in place.

11. **Do we have any SSR requirements on the physical site visit in the case of cloud vendors?** You need to update the narrative data flow. You should also accurately fill out the cloud computing section by describing how you engage with the vendor and the protections. You don't need to provide a site visit or physical assessment of the cloud vendor because you have no way to do that.

12. **If data is fully encrypted, passes through a cloud vendor and is not stored, does this still require the vendor to be FedRAMP certified?** Yes, it does. Any system that receives, transmits, processes or stores FTI is in scope, and even if the vendor encrypts FTI, all the protections around FTI apply to that data

13. **It is my understanding that IRS prohibits any contractor to have access to FTI. Does that requirement remain the same in cloud implementation?** Yes, the requirement applies regardless of where FTI goes. Maintaining encryption keys for data at rest and in transit isolates the cloud vendor from having logical access to the data.

14. **Is the cloud vendor not able to use support staff outside the U.S. to support their cloud? How would agencies verify this?** Many vendors actively market their solutions. Agencies must research how the cloud provider handles system administration during procurement of the service. Larger cloud vendors have reached different levels of authorization (high, moderate or low) and may be able to assure the government that they have no offshore access.

15. **How would it be possible for an agency to maintain the encryption keys for TLS connections?** Agencies primarily need to maintain keys for the data encrypted at rest (should only be able to be deciphered by the agency). Agencies don't specifically need to be the sole owner of data in transit; but, the vendor shouldn't be able to gain access to data in transit or at rest.

16. **Has any cloud provider not allowed IRS to use applicable SCSEMS citing attestations and/or independent third-party audits?** This hasn't happened because of how Safeguards scopes assessments for cloud solutions. Safeguards only assesses the types of security controls the agency has primary responsibility for carrying out. Safeguards staff doesn't physically go to FedRAMP authorized facilities.

17. **What is the position of O365 and how it pertains to the restriction of not accessing it via the internet?** The agency may access it through the agency's dedicated network. The agency may also access it through a mobile phone that's part of a Mobile Device Management solution, so the agency can carry out proper access controls to protect FTI traversing through the device.