Office of Safeguards

March 2022 Office Hours – Top Technical Inquiries (TI)

March 15, 2022
March 17, 2022

Top Technical Inquiries (TI) Overview 2014-2021

IRS Office of Safeguards identified the top three TIs and their frequency…

119
33

The cloud computing environment is not configured securely
and
Encryption capabilities do not meet Federal Information Processing Standards (FIPS) 140 requirements

29

Contractor access to federal tax information (FTI)

37

Clarification on Significant Corrective Action Plans (CAP) findings

TI: “cloud computing environment is not configured securely” and “encryption capabilities do not meet FIPS 140 Requirements”

Cloud Computing Environment

- What are the requirements for implementing a cloud computing environment?
- How far in advance should an agency submit a cloud computing notification before planned implementation?
- Which cloud environments are approved?

Encryption Capabilities

- Is 7-Zip an IRS approved encryption method?
- Are there any specific rules (e.g., type certificates, minimum length, encryption, etc.) for new, renewed Secure Sockets Layer (SSL) certificates?

Responses to “cloud computing environment is not configured securely”

- IRS requirement for Cloud Computing is located on the Office of Safeguards website:
  - https://www.irs.gov/privacy-disclosure/cloud-computing-environment
- The agency must notify the IRS Office of Safeguards at least 45 days before transmitting federal tax information (FTI) into a cloud environment
- Only FedRAMP authorized (moderate/high impact) cloud service offerings are accepted by the Office of Safeguards.
  - FedRAMP isn't the only requirement.
  - Safeguards does not approve cloud notifications, we accept them.
  - Use this link for info: https://marketplace.fedramp.gov/#!/products?sort=productName&status=Compliant

Responses to “Encryption Capabilities do not meet FIPS 140 Requirements”

- 7-Zip is not an approved IRS encryption method
  - The IRS Office of Safeguards can’t receive files with the .7z extension for submitted reports. The IRS will accept .zip and .zipx encrypted files. IRS Publication 1075 (11-2021) Section 2.E provides more guidance.
- The National Institute of Standards and Technology (NIST) maintains a list of validated cryptographic modules on its website: http://csrc.nist.gov/
- All internet transmissions must use FIPS compliant cryptography
  - Transport Layer Security (TLS/SSL) must be version 1.2 or later (See NIST SP 800-52R2 for more details)
  - NIST provides recommendations for other algorithms in NIST SP 800-131AR2, including:
  - AES (128, 192, 256)
  - RSA (≥2048)

TI: Cloud Computing Environment and Encryption Capabilities

Find the answers in Publication 1075…

- Pub 1075 (Rev. 11-2021): Publication 1075 (Rev. 11-2021) (irs.gov)
  - 3.3 Technology-Specific Requirements, 3.3.1 Cloud Computing
  - 2.E.3 Encryption Requirements
  - IA-7: Cryptographic Module Authentication
  - SC-12: Cryptographic Key Establishment and Management
  - SC-13: Cryptographic Protection
  - SC-17: Public Key Infrastructure Certificates
  - SC-28: Protection of Information at Rest

TI: “contractor’s access to FTI...”

IRS Office of Safeguards has highlighted common questions that may arise in response to contractor’s access when related to FTI:

- How does an agency know when to file a 45-day contractor notification with the Office of Safeguards?
- What are the requirements for contractors and subcontractors of agencies that receive, process, store, access, protect and/or transmit FTI?
- During data migrations to clouds, does the agency need to file a 45-day Live Data Testing Request Notification if the cloud vendor will not have logical access to FTI?

Responses to TI related to “contractor access to FTI...”

- If an agency receives, processes, stores, accesses, protects and/or transmits FTI with the help of contractors with logical or physical access to FTI:
  - Then the agency must File a 45-day Contractor Notification with the IRS Office of Safeguards.
- If an agency receives FTI under authority of IRC section 6103(l)(7) (human services agencies)
  - Then the agency may not disclose FTI to contractors for any purpose.
- If the contractor doesn’t have logical or physical access to FTI at any point during a data migration
  - Then a 45-day Live Data Testing Request Notification doesn’t need to be filed. But an approved Cloud Computing Notification should be on file with the Office of Safeguards before FTI being received, processed, stored, accessed, protected; and/or transmitted to the cloud environment.
- If contractors are used
  - Then a contract/SLA is needed between the agency authorized to receive FTI and support functions. If contractors are authorized access, then the contract between the agency and the contractor must include language from Exhibit 7, Safeguarding Contract Language. As part of the agency review process, all affiliated contractors and subcontractors who receive, transmit, process and store FTI on behalf of the agency are subject to review and testing.
- Contractors include:
  - Cloud service providers, consolidated data centers, off-site storage facilities, disposal companies, information technology support, or tax modeling or revenue forecasting providers.

TI: “contractor access to FTI”

Find answers in specific sections of Publication 1075

- Pub 1075 (Rev. 11-2021): Publication 1075 (Rev. 11-2021) (irs.gov)
  - 2.C.8.2 Agency, Contractor or Sub-Contractor Shared Facilities
  - 2.C.9 Service Level Agreements (SLA)
  - 2.C.10 Review Availability of Contractor and Sub-Contractor Facilities
  - 2.E.6.2 Contractor or Sub-Contractor Access
  - Exhibit 6 Contractor 45-Day Notification Procedures
  - Exhibit 7 Safeguarding Contract Language

TI: “Clarification on Significant CAP Findings…”

IRS Office of Safeguards has highlighted common questions and concerns that may arise in response to CAP findings:

- H.3.10 - Review security audit logs at least weekly for indications of unusual activity. This was identified for multifunctional devices (printer).
  - Access to the printer is restricted to authorized users only, per division policy. The agency would like clarification on what information the Office of Safeguards needs for the security audit log?
- H.17.1 - Access to the data warehouse manager and the individual FTI data stores are not restricted to authorized agency personnel with a valid need-to-know and a job function that requires access to FTI.
  - We understand the finding is about the COTS web application; but we're not sure what "data warehouse manager" in the finding is referring to.
- IRS Pub 1075 - “Provide evidentiary documentation to validate the closure of any findings identified as critical or significant.”
  - Could the Office of Safeguards describe the documentation expected?

Responses to TI's related to "clarification on significant CAP findings..."

- H.3.10 - The agency should update the process documentation that addresses and governs auditing for the device and ensure that security audit logs are reviewed weekly for activity related to potential unauthorized FTI access.
  - IRS Publication 1075 addresses the types of activity that should be monitored as well as how to report events. This function may be done by a security group or audit group with responsibility for maintaining and analyzing system audit logs.
- H.17.1 - The data warehouse manager was mentioned in this finding because it stores the data from the application. Two separate Safeguard Computer Security Evaluation Matrix (SCSEMS) apply to COTS Web Application and the enterprise data warehouse.
  - Finding H17.1 is only associated with the COTS web application. This test case is to determine which user profiles give access to the backend administrator tool through the UI Group "SysUtil." To close this finding, the agency can provide screenshots of the users with access to the UI Group "SysUtil" and screenshots of the administrators for the COTS web application confirming that only administrator level users have backend access to the COTS application.
- IRS Pub 1075 - Critical and significant findings require evidence such as policies, procedures, scan results and screenshots that shows remediation of the specific finding and ties to the system identified in the CAP.

TI: clarification on significant CAP findings

Find answers in specific sections of Publication 1075

- Pub 1075 (Rev. 11-2021): Publication 1075 (Rev. 11-2021) (irs.gov)
  - AU-6: Audit Review, Analysis and Reporting
  - AC-3 Access Enforcement
  - Table 3 – Safeguard Security Report (SSR) Evidentiary Documentation
  - 2.E.5.1 CAP Submission Instructions

Q&A