Office of Safeguards

Guidance on Live Data and Cloud Computing Requests

February 2021 Office Hour Call

Agenda

- Introduction
- Reporting Requirements – IT notifications
  - Cloud Computing
  - Live Data Testing
- Notification Process Flow
- Forms
- Summary
- References

Introduction

- IRC 6103 limits the use of federal tax information (FTI) to certain purposes based on the authority under which received.
- Due to security, risk of unauthorized disclosure and use of FTI, Safeguards requires notification 45 days before implementing certain operations or technology capabilities that use FTI.
- There are additional circumstances or technology implementations that require agencies to submit notification to the Office of Safeguards (e.g., Disclosure to a Contractor), at a minimum of 45 days ahead of the planned implementation. Please reference, Pub 1075 Section ***7.4 45-Day Notification Reporting Requirements*** for a complete list.
- This Office Hours session will focus on processing IT notification forms for these activities involving FTI:
  - Cloud Computing: receiving, processing, storing or transmitting FTI in a cloud environment
  - Live Data Testing: use of live FTI in a testing environment

Cloud Computing Requirements

- The agency must comply with the following requirements

Requirement	Description	Additional Information
Notification Requirement	The agency must notify the Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment.	• https://www.irs.gov/privacy-disclosure/cloud-computing-environment • Publication 1075: Section 9.4.1 Cloud Computing Environments.
FedRAMP Authorization	Agencies maintaining FTI within cloud environments must engage services from FedRAMP certified vendors to complete the authorization framework resulting in an Authority to Operate.	https://marketplace.fedramp.gov/#!/products
Onshore Access	Agencies must leverage vendors and services where (i) all FTI physically resides in systems located within the United States; and (ii) all access, and support of such data is performed from the United States.	There is no access to FTI (personnel or FTI systems/equipment) or the cloud technology from offshore locations.
Physical Description	Agencies and their cloud providers must provide a complete listing of all data centers within the cloud environment where FTI will be received, processed, transmitted or stored. Agency must describe the system architecture and business functions for using the cloud.	https://www.irs.gov/privacy-disclosure/cloud-computing-environment
Data Isolation	Software, data, and services that receive, process, store, or transmit FTI must be isolated within the cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications.	Who manages access control for data in the cloud? • FTI cannot be shared with other cloud tenants. • FTI must only be disclosed to other organizations per IRC 6103(p)(4). • Account access must follow Need to Know and Least Privilege best practices.

Cloud Computing Requirements cont'd.

- The agency must comply with the following requirements

Requirement	Description	Additional Information
Service Level Agreements (SLA)	The agency must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled, and accessed inside the cloud through a legally binding contract or SLA with its third-party cloud provider.	• Does the SLA with the Cloud Provider cover all requirements? • SLA must comply with requirements stated under Section 5.5.2 and Exhibit 7 of IRS Publication 1075. • SLA must state how the cloud provider will dispose of storage assets containing FTI. • SLA must identify the cloud service model procured by the agency to help define agency-managed controls.
Data Encryption at Rest	FTI must be encrypted while at rest in the cloud. All mechanisms used to encrypt FTI must use the latest FIPS 140 compliant module. This requirement must be included in the SLA, if applicable.	Agency must specify the latest FIPS 140 compliant algorithms implemented (i.e AES, 3DES with at least 128 bits in strength) to encrypt FTI at rest.
Persistence of Data in Relieved Assets	Storage devices where FTI has resided must be securely sanitized and/or destroyed using methods acceptable by National Security Agency/Central Security Service (NSA/CSS). This requirement must be included in the SLA.	The agency needs to explain what media will contain FTI and the process to sanitize and dispose of media when it is no longer needed.

Cloud Computing Requirements

- The agency must comply with the following requirements

Requirement	Description	Additional Information
Risk Assessment	The agency must conduct an annual assessment of the security controls in place on all information systems used for receiving, processing, storing, or transmitting FTI. For the annual assessment immediately prior to implementation of the cloud environment and each annual risk assessment (or update to an existing risk assessment) thereafter, the agency must include the cloud environment. The Office of Safeguards will evaluate the risk assessment as part of the notification requirement in Requirement (a.).	• How does the agency assess risk of cloud implementation? • Periodic agency assessment must include magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of FTI and cloud systems.
Remote Access	Remote access is defined as any access to an agency information system by a user communicating through an external network, for example, the Internet. FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore—outside of the United States territories, embassies, or military installations. Further, FTI may not be received, processed, stored, transmitted, or disposed of by IT systems located offshore.	• Access to the cloud should be routed through the agency's network. • Direct access to the cloud must occur after multi-factor authentication. • Any remote access where FTI is accessed over the remote connection must be performed using multi-factor authentication.

Live Data Testing Requirements

- IRS Publication 1075 requires agencies to submit a Live Data Request form at least 45 days prior to intended use.
- The request must explain safeguards in place to protect data and the need for using live data during testing.
- Critical control areas from Publication 1075 include:

Requirement	Description	Additional Information
Physical Security Controls	The area where the test systems are stored must meet minimum protection standards outlined in Publication 1075, which includes two barriers to access FTI under normal security.	This item is looking for defense in-depth or Gates, Guards; physical measures in place to protect the systems that process, store, transmit, or receive FTI data. Examples include, but not limited to: • Guards (24/7) • Badge access
Logical Access Controls	The agency must ensure that only authorized employees or contractors (if allowed by statute) of the agency receiving the information have access to the system with FTI, and that user accounts for the test systems are managed according to production system standards for establishing, activating, changing, reviewing, disabling and removing accounts.	This security item requires the agency describe logical access. Examples include, but not limited to: •Active Directory •Security groups (role-based access) •Agency needs to specifically state whether remote access is allowed; if so, Multi-Factor Authentication (MFA) must be in place •VPN

Live Data Testing Requirements

- Critical control areas from Publication 1075 include:

Requirement	Description	Additional Information
Identification and Authentication	The test system must be configured to uniquely identify users, devices and processes via the assignment of unique user accounts and authentication methods such as passwords, tokens, smart cards, etc.	This security item requires agencies describe how users / staff are identified and authenticated to the information system. Examples include, but not limited to: • Authentication solution (Active Directory) • Password Parameters (IRS Pub 1075 requirements)
Data Labeling	If FTI is commingled with other state data, the FTI must be labeled at the data element level to identify it as FTI at all times. This includes data that may be commingled within a database or data warehouse.	FTI must be clearly labeled and handled in such a manner that it does not become misplaced or available to unauthorized personnel.
Audit and Accountability	The test system must generate a level of audit records to the extent necessary to capture unauthorized access of FTI by unique users. As part of system testing, the agency should try to mimic the audit capabilities that will be in place in production to ensure auditing functions properly.	This security item requires agencies describe their audit and accountability capabilities. Examples include, but not limited to: 1. 7-year retention 2. Description of what activities are audited / collected per IRS Pub 1075 3. Log in / log off; to include Successful / unsuccessful logins 4. Modification, deletion, addition to tables 5. Access times

Live Data Testing Requirements

- Critical control areas from Publication 1075 include:

Requirement	Description	Additional Information
Encryption	All FTI in transit must be encrypted when moving across a Wide Area Network (WAN) and within the agency's Local Area Network (LAN).	This security item requires agencies describe solution in place to protect FTI in transit. Examples include, but not limited to: • TLS version 1.2 and higher (if the agency is not using version 1.2 or higher, ask the agency plans for upgrading) • HTTPS • Any FIPS compliant and/or enabled solution must be listed / describe if not one of the above
Incident response and reporting	The agency must follow the incident response and reporting procedure used for production systems for any incident involving FTI that occurs on a test system. This includes notification to the Office of Safeguards and TIGTA no later than 24 hours after the identification of a possible incident. System testers are trained and aware of the incident response process.	The agency must specifically state that all incidents involving FTI will be reported to TIGTA and the IRS Ofc of Safeguards within 24hrs.
Contractor Access	Agencies must follow the regulations in the statute for disclosing FTI to a contractor. For agencies that utilize a contractor, the Safeguarding language must be included in their contract, the agency must provide notification to the IRS 45 days prior to the contractor having access to FTI, all contractor staff must have a background investigation initiated, and the contractor must be trained on both disclosure awareness and incident response.	

Live Data Testing Requirements

- Critical control areas from Publication 1075 include:

Requirement	Description	Additional Information
Limited Timeframe	IRS approval for on-going testing is valid for three years from the date of the approval. If the agency needs to continue the use of FTI in pre-production testing activities past the three-year timeframe, a new request for live data must be submitted to the IRS.	
Reporting	The agency must notify the IRS a minimum of 45 days prior to moving FTI to the pre-production environment and update their SSR section 9.4.6. If the annual SSR has already been submitted the agency must report the testing the following year. Additionally, for approved on-going testing efforts the agency must report any changes to their pre-production environment or uses of the FTI in the pre-production environment that was not previously covered in the request for live data with a new submission.	
Sanitization and Disposal	Agencies must follow data sanitization and disposal procedures in accordance with Publication 1075 once the FTI is no longer needed in the test environment. For one-time testing efforts agencies must delete the data from the test system and clear the system's hard drive prior to repurposing the system for other state agency testing efforts. For on-going testing efforts, the FTI may remain on the system for the duration of the approved testing timeframe, however once the approved testing timeframe expires, the agency must delete the data from the test system and clear the system's hard drive prior to repurposing the system for other state agency testing efforts; or submit a new request for live data testing to the IRS.	

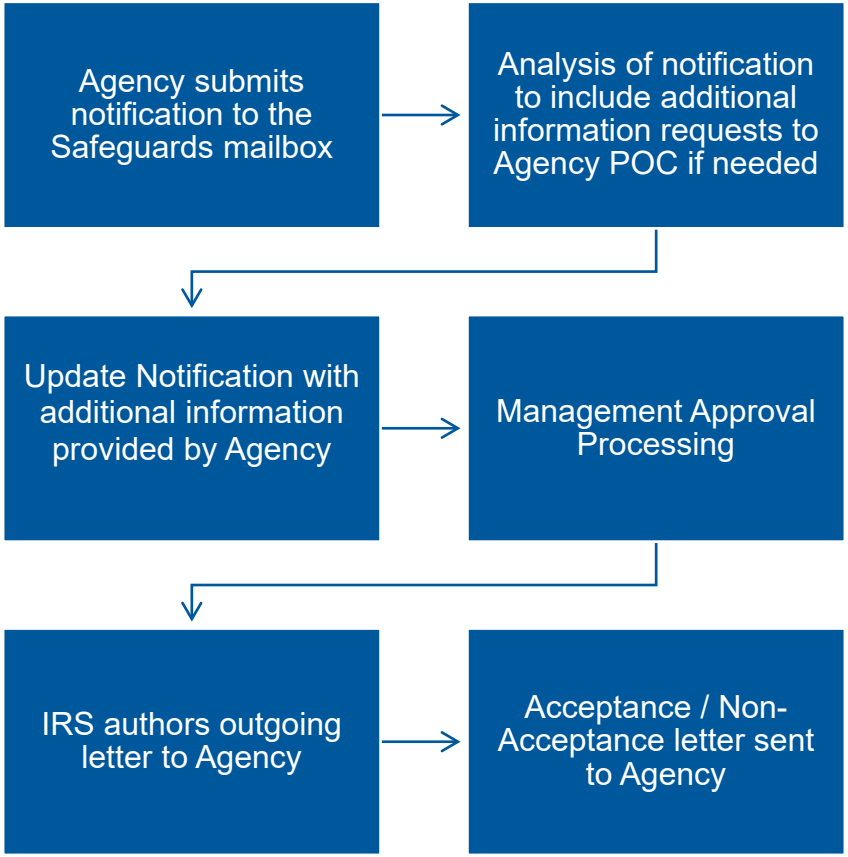
Live Data Testing Requirements

- Critical control areas from Publication 1075 include:

Requirement	Description	Additional Information
Remote Access	Remote access is defined as any access to an agency information system by a user communicating through an external network, for example, the Internet. FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore—outside of the United States territories, embassies, or military installations. Further, FTI may not be received, processed, stored, transmitted, or disposed of by IT systems located offshore.	• Agency needs to specifically state whether remote access is allowed; if so, Multi-Factor Authentication (MFA) must be in place.
Offshore Access	FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore—outside of the United States territories, embassies, or military installations. Further, FTI may not be received, processed, stored, transmitted, or disposed of by IT systems located offshore.	• The agency needs to confirm FTI will not be accessed from offshore locations. • Agency personnel may not receive, process, store or transmit FTI in offshore locations.

Notification Process Flow

- Our goal is to respond to all Notification requests within 30 days of receipt.



LDTR and Cloud Notification Forms

- Please be sure to only complete the most update to date version of the notification forms. Old forms that are submitted by an agency will not be processed.

Cloud Computing Form

LDTR Form

Cloud Computing Form

LDTR Form

(when in the cloud)

Summary

- To avoid delays, ensure the following:
  - Address and respond to each security control
  - Include the data center addresses for cloud environments
  - Provide the full scope of the testing environment to include operating system version(s) and software version(s), boundary protections, workstations used to access the data, etc
- To receive IRS approval, at a minimum, meet the following criteria:
  - No out-of-support devices and no off-shore access
  - No cloud solutions without FedRAMP authorization of moderate or high level
  - No unauthorized disclosure
  - Enable MFA for remote access
  - Encrypt FTI in transit and at rest (when in the cloud) using the latest FIPS certified encryption
  - No logical access to FTI from the cloud vendors
  - Audit logs are generated and reviewed at least weekly
- Notify the IRS a minimum of 45 days before moving FTI to the preproduction environment and/or cloud systems.

Summary

- Update SSR Section 9.4.6. If you already submitted the annual SSR, report the testing the following year.
- Review IRS Publication 1075 for all notification reporting requirements and instructions on completing forms.
- The Dev/Test environment must have the same level of robust security controls as Production.

References

- IRS Publication 1075
  - *7.4 45-Day Notification Reporting Requirements*
  - *Exhibit 6 Contractor 45-Day Notification Procedures*
- Office of SGs Cloud Computing Requirements
- Office of Safeguards Live Data Testing Requirements
- Office of SGs 45-day notification requirements
- FedRAMP Service Providers