Internal Revenue Service (IRS)

Office of Safeguards

Live Data Testing Request Form

**June 2020**

# Introduction

Per IRS Publication 1075, agencies must submit a request to the IRS Office of Safeguards for authority to use live FTI data for testing. This request must include a detailed explanation of the safeguards in place to protect the data and the necessity for using live FTI data during testing. The intent of this form is to document environments where FTI resides but is not subject to the same level of security controls as the production system(s).

# How to Complete This Document

Agencies should review the security controls and compliance inquiries included below and provide their complete response in Part 1 of the form. This is a standalone form and it needs to stand on its own. Please ensure that all information is written out to address each control. **The IRS cannot accept any responses that reference other documents this includes but not limited to SSR, Agency Policy and Procedures, NIST, etc.** However, this information may be transposed into this document.

All submissions should be sent to the IRS Safeguards mailbox ([SafeguardReports@irs.gov](file:///C:\Users\BKKDB\AppData\Local\AppData\Local\Microsoft\AppData\Local\Microsoft\Windows\SBU%20Data\Outlook%20Data\SafeguardReports@irs.gov)) with the subject line: **Live FTI Data Request**. The information requested through this document is not meant to be all-encompassing and the IRS may require additional information from the agency in order to evaluate the planned data warehouse implementation.

# Document Workflow

The IRS will evaluate the agency’s submission and complete Part 2 of the form. Upon submission of the table below, agencies may be contacted by the IRS to schedule a conference call for the IRS for additional information or discussion based upon the specific facts provided.

**Documentation Requirements**

| **Live Data Testing Notification Form – Part 1** | |
| --- | --- |
| **Date:** |  |
| **Agency:** |  |
| **POC Name:** |  |
| **POC Title:** |  |
| **POC Phone / Email:** | [Please use this format (XXX) XXX-XXXX / E-Mail] |
| **POC Site / Location:** |  |
| **Site / Location FTI:** |  |

|  |  | |
| --- | --- | --- |
| **#** | **Compliance Inquiry** | **Agency Response** |
| **1** | Site / Location of FTI: | [**Note:** Please be as detailed as possible in your responses. All responses must be in **BLACK** font. Please do not change the format of the document or orientation.]  Agency must detail all physical locations where FTI will reside in the test system |
| **2** | FTI Data Extract Requested for Use in System Testing  [**Note**: Please provide specific extracts and or data element information] | The agency should list all FTI data extracts that will be used during testing and evaluation |
| **3** | Application / System Name | Custom or COTS Application name and version |
| **4** | Describe the Proposed Use of FTI in Pre-Production System Testing (e.g., what type of testing will be performed, why live data needs to be used instead of dummy data)  [**Also:** Please justify the business case in detail. Highlight areas where the controls in the test environment differ from the production environment.] | Agency needs to clearly explain the reason they require using live FTI data as opposed to synthetic data  Agency should describe the business process the system allows to function, e.g., case management, data warehousing, tax processing, benefits administration, etc..) |
| **5** | Provide a narrative data flow to include complete list of all devices / systems in the development and/or test environment that will receive process, store or transmit FTI. Include a data flow diagram.  [**Note:** Please include the make, model, firmware, and software for all hardware and software components (e.g., RHEL 6.7, SQL 2016). The agency should also state if the servers are physical or virtual; if servers are virtual, the agency needs to specify the hypervisor name (i.e. ESXi) and version number.] | Details to include:   * Operating System Versions for web, application, and database servers(e.g., Windows 2019, Red Hat Enterprise Linux version 7.8) * Databases – Oracle 12c, MS SQL 2014 SP3, Adabas, database webserver level, development environment, .net., java. etc. * If mainframe – need IBM z/OS version along with the name of the security suite (RACF, ACF2) and version * Make, model, and firmware versions of perimeter protection devices and remote access mechanisms * Need version of all web server software (e.g., IIS version 8, Apache 2.4.29) * Versions of hypervisors and SAN firmware versions * Transmission protocols for how FTI is transferred into the test environment (e.g., SFTP) and how it is accessed (e.g., HTTPS, encrypted DBMS client, etc.) |
| **6** | **Testing/Validation Period:**   1. Will the FTI be used for a one-time testing effort (e.g., system testing that is done prior to a new system implementation), or an on-going testing effort? 2. Provide the start date and end date that FTI data will be used.   **[Note:** 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.] | Agency needs to specify one-time or on-going testing effort along with the date or dates of testing period; the Office of Safeguards grants approvals in 3-year increments.   1. The testing will be for an on-going testing and system validation effort. 2. 07/10/2020 – 07/10/2023 |
| **7** | **Contractor Info:**  If contractors will have access to FTI in the pre-production test environment, please state what role the contractors will have in testing. In addition, please provide the name of the company, the number of contractors that will access FTI, and the location at which the testing work will be completed.  [**Note:** FTI may not be accessed by agency employees, agents, representatives or contractors located “offshore”, outside of the United States or its territories. Further, FTI may not be received, stored, processed or disposed via information technology systems located offshore. | **Name:**  **Number of Contractors Accessing FTI:**  **Location of Testing:**  **Purpose:**  **Awareness and Confidentiality:**  **Exhibit 7 Language:**  **Offshore:** (Yes or No)  **State Run Datacenter:** (Yes or No) |
| **8** | Describe the Controls in Place to Protect FTI in Pre-Production System Test Environment (specifically address at a minimum the areas listed in the Live Data Testing Memo)   * + Physical Security Controls   + Logical Access Controls   + Identification and Authentication   + Audit and Accountability   + Labeling   + Encryption of FTI in Transit and at rest   + Incident response and reporting   + Sanitization and Disposal   + Contractor Access   + Notification for Data Warehouse   + Reporting (SSR Update) | [**Note:** If the controls are similar to production detail them out below, please don’t state that the development controls are similar to production. Also, the IRS cannot accept any responses that reference other documents this includes but not limited to SSR, Agency Policy and Procedures, NIST, etc. Lastly, please be as comprehensive as possible in your responses.] |
| **8a** | **Physical Security Controls:**  **[Note:** Examples include, but not limited to guards (24/7), CCTV, badge access, auditing etc.] | This item is looking for physical safeguards or a defense in-depth physical measures in place to protect the systems that process, store, transmit, or receives FTI data. |
| **8b** | **Logical Access Controls**  Please describe processes for how users are granted access to the test environment. If remote access is allowed to the test environment, describe the multifactor authentication solution(s) including all potential factors for gaining access. | This item is looking for access controls which intend to limit access to the test environment. Include authorization processes for accounts, system timeout configurations, warning banners, etc. |
| **8c** | **Identification and Authentication:**  Please describe how users/staff are identified and authenticated into the system.  [**Note:** Examples include an authentication solution (Active directory), password parameters, 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 (e.g., Active Directory) * Password Parameters (should meet IRS Pub 1075 requirements) |
| **8d** | **Audit and Accountability:**  Please describe/list all the auditable events (i.e., successful / unsuccessful login, access times, etc.) that will be tracked by the database, OS, or application  [**Note:** Please specify if audit records are retained as required by IRS Publication 1075.] | This security item requires agencies describe their audit and accountability capabilities. Examples include, but not limited to:   * 7 year retention; * Description of what activities are audited / collected (per IRS Pub 1075); * Log in / log off; to include Successful / unsuccessful logins; * Modification, deletion, addition to tables; * Access times * Discussion of incorporation of events into a SIEM tool * Refer to IRS Publication 1075, Section 9.3.3.2 Audit Events (AU-) for a more extensive list of events types |
| **8e** | **Labeling:**  If FTI will be tested in a database or data warehouse, indicate the type of database (including specific name and version number) or data warehouse.  [**Note:** Please provide a detailed explanation about how FTI data elements will be labelled within the database or data warehouse. Tables containing FTI should be labeled with identifier such as (e.g., TAX, FTI, IRS, etc.). If FTI is commingled with other state data, the FTI must always be labelled at the data element level to identify it as FTI. If FTI is not commingled within a table, the FTI must be labeled at the table level, or at the database level if a database is dedicated to FTI data.] | This security item requires agencies explain how FTI is labeled for identification when commingled with other standard agency data.   * Database / Datawarehouse * Is FTI commingled (Yes/No): Yes * FTI is labelled with a unique identifier |
| **8f** | **Encryption of FTI in Transit and Data at Rest:**  Please specify the encryption name, make, and version number of the specific protocols (algorithms, ciphers, AES256, etc..) that will be used to establish encryption.  [**Note:** Encryption must be FIPS 140-2 compliant and the agency should maintain sole ownership of encryption keys] | This security item requires agencies describe solution in place to protect FTI in transit. Examples include, but not limited to:   * Version of TLS protecting the transport layer * Symmetric encryption algorithm to include key length (e.g., AES-128); * Any FIPS compliant and/or enabled solution must be listed / describe if not one of the above |
| **8g** | **Incident response and reporting:**  Please state or provide your agency’s policy involving FTI incidents.  [**Note:** Office of Safeguards and TIGTA must be notified, no later than 24 hours, after the identification of a possible incident] | The agency must specifically state that all incidents involving FTI will be reported to TIGTA and the IRS Ofc of Safeguards within 24hrs. |
| **8h** | **Sanitization** **and Disposal:**  Please describe your data sanitization process.  [**Note:** 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.] | The agency must describe how it will sanitize the test environment at the end of the test period. |
| **8i** | **Reporting (SSR Update):**  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.  [**Note:** 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.in the request for live data.] |  |
| **8j** | **Backup and Contingency Planning:**  Describe how backups are handled, including what is backed up, to what is it backed up, according to what frequency, and where is it being stored (e.g. tapes, NAS, Storage Area Network (SAN)). | The agency must specify whether backups are being performed, frequency and what type of media is being used to store FTI logs and FTI data. Additionally, the Agency should provide the name of the backup / storage solution and version.   * DELL EMC SAN version 3.4 * Data is encrypted (AES256) as its being transmitted to the SAN and while it’s at rest (AES256) |

|  |  |  |  |
| --- | --- | --- | --- |
| **Live Data Testing Notification Form – Part 2** | | | |
| **Date:** | |  | |
| **Reviewer’s Name:** | |  | |
| **Approval Decision:** | |  | |
|  | | **Comments** | |
| **#** | **IRS Comments** | | **Agency Response** |
| **1** | For items below we need clarification on, please comment in blue font (see 10a). The agency should provide their response in the ‘Comments’ section adjacent to item number. | | **Agency Response, Date X/XX/2014:**  Note: Please update the date above and place your response here. Please follow this format for the remainder of the document. |
| **2** |  | |  |
| **3** |  | |  |
| **4** |  | |  |
| **5** |  | |  |
| **6** |  | |  |
| **7** |  | |  |
| **8a** |  | |  |
| **8b** |  | |  |
| **8c** |  | |  |
| **8d** |  | |  |
| **8e** |  | |  |
| **8f** |  | |  |
| **8g** |  | |  |
| **8h** |  | |  |
| **8i** |  | |  |
| **8j** |  | |  |