IRS PUB 1075
Tax Information Security Guidelines For Federal, State and Local Agencies
Summary

Developed By Karen Y. Baez

Publication 1075 Overview

This updated publication…

- Provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, contractors, or sub-contractors adequately protect the confidentiality of FTI. Enterprise security policies address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance to implement all applicable security controls.

- Provides a breakdown of the managerial, operational, and technical security controls that must be implemented as a condition of receipt of FTI. The guidelines outlined herein apply to all FTI, no matter the amount or the media in which it is recorded. FTI must be afforded the same levels of protection regardless of it residing on paper or electronic form. Systematic, procedural, or manual security policies must minimize circumvention. A mutual interest exists in our responsibility to ensure that FTI is disclosed only to persons authorized and used only as authorized by statute or regulation.

- Provides the preliminary steps to consider before submitting a request to receive FTI, requirements for proper protection, expectations from the IRS and considerations that may be helpful in establishing a program to protect FTI. The exhibits in this publication are provided for additional guidance

What is FTI?

FTI stands for Federal Tax Information. Safeguarding FTI is critically important to continuously protect taxpayer confidentiality as required by IRC § 6103.

- FTI consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control that is covered by the confidentiality protections of the IRC and subject to the IRC § 6103(p)(4) safeguarding requirements including IRS oversight.
- FTI is categorized as Sensitive But Unclassified (SBU) information and may contain personally identifiable information (PII).
- FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS) or Centers for Medicare and Medicaid Services (CMS) or another entity acting on behalf of the IRS pursuant to an IRC § 6103(p)(2)(B) Agreement.
- FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

What is the IRS FIPS Security Categorization Level for FTI Data?

MODERATE

Why is safeguarding FTI important ?

Safeguarding FTI is important because…

- IRS must foster a tax system based on voluntary compliance, so the public can have a high degree of confidence that the personal and financial information furnished to the Internal Revenue Service (IRS) is protected against unauthorized use, inspection, or disclosure.
- In lieu of the above, the IRS must administer the disclosure provisions of the Internal Revenue Code (IRC) according to the spirit and intent of these laws, ever mindful of the public trust. To do so, the IRC defines and protects the confidential relationship between the taxpayer and the IRS and makes it a crime to violate this confidence.
  - IRC § 7213 prescribes criminal penalties, making it a felony offense for federal and state employees and others who illegally disclose federal tax returns and return information (FTI).
  - IRC § 7213A makes the unauthorized inspection of FTI a misdemeanor, punishable by fines, imprisonment, or both.
  - IRC § 7431 prescribes civil damages available to the taxpayer upon notification that a criminal indictment or the existence of information that an unauthorized inspection or disclosure has occurred under IRC §§ 7213 or 7213(A).
- The concerns of citizens and Congress regarding individual rights to privacy require the IRS to continuously assess disclosure practices and the safeguards used to protect the confidential information entrusted. While the sanctions of the IRC are designed to protect the privacy of taxpayers, the IRS recognizes the importance of cooperating to the fullest extent permitted by law with other federal, state, and local authorities in their administration and enforcement of laws.

Who must comply with this publication?

ANY AGENCY OR AGENT legally handling or receiving FTI directly from the IRS or secondary sources (e.g., Social Security Administration [SSA], pursuant to IRC § 6103 or by an IRS-approved exchange agreement.

ANY Contractor or Sub-Contractor Services procured by the agency to handle FTI on its behalf.

Can agencies share FTI and associated reports?

IRS Safeguards reports and related communications in possession of federal, state, and local agencies are considered the property of the IRS and may not be disclosed to anyone outside the agency and are subject to disclosure restrictions under federal law and IRS rules and regulations. This includes, but is not limited to, Preliminary Findings Report (PFR); Safeguard Review Report (SRR); Safeguard Security Report (SSR) and Corrective Action Plan (CAP). IRC § 6103 is a confidentiality statute and generally prohibits the disclosure of FTI.

Release of any IRS Safeguards document requires the express permission of the Internal Revenue Service. Requests received through Sunshine and/or Information Sharing/Open Records provisions must be referred to the federal Freedom of Information Act (FOIA) statute for processing. State and local agencies receiving such requests must refer the requestor to the instructions to file a FOIA request with the IRS.

Federal agencies must follow established procedures that require consultation before citing FOIA exemptions on IRS agency records, or directly refer the FOIA request to IRS for processing. The intent of this requirement is to address any public request for sensitive information and prevent disclosure of data that would put FTI at risk. The agency may still distribute these reports internally and within other state agencies, or to auditors or oversight panels as required to either take corrective actions or report status without further IRS approval.

NOTE: Additional guidance may be found at, https://www.irs.gov/uac/IRS-Freedom-of-Information, and questions should be referred to the Safeguards mailbox at Safeguardreports@irs.gov.

Are there any exceptions for sharing FTI?

YES

Exceptions to the general rule authorize disclosure of FTI to certain federal, state, and local agencies. Generally, these disclosures are made by the IRS in response to written requests signed by the head of the requesting agency or an authorized delegate. However, the agency must…

- Used FTI solely for the purpose described in the exception authorizing the disclosure. The statutes providing authorization to disclose FTI contain specific conditions that may require different procedures in maintaining and using the information.
- Demonstrate, to the satisfaction of the IRS, the ability to protect the confidentiality of that information. Certain safeguards must be implemented to prevent unauthorized access and use. Besides written requests, the IRS may require formal agreements that specify, among other things, how the information will be protected.
- Ensure its safeguards will be ready for immediate implementation upon receipt of FTI. Copies of the initial and subsequent requests for data and any formal agreement must be retained by the agency a minimum of five (5) years as a part of its recordkeeping system. Agencies must always maintain the latest SSR on file.
- Submit must submit a SSR to Safeguards at least 90 days before the scheduled or requested receipt of the initial FTI request (see Section 2.E, Reporting Requirements—6103(p)(4)(E)). The SSR must include processing and safeguard procedures for all FTI received and distinguish between agency programs and functional organizations using FTI.
- Consolidate Multiple organizations, divisions or programs within a federal agency using FTI must be consolidated into a single report for that agency at the direction of Safeguards. Agencies entering into an agreement to disclose FTI to agents, contractors, or sub-contractors requires advance notice to IRS Safeguards (see Section 2.E.6 Notification Reporting Requirements and Section 1.9.4, Disclosing FTI to Contractors or Sub-Contractors.)

FTI General Requirements

Overview

What's deemed authorized FTI use?

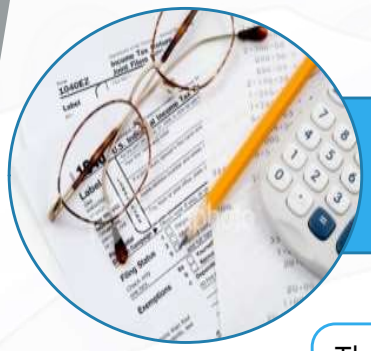
AUTHORIZE FTI USE is strictly limited to the request submitted and approved by IRS and limited to the purpose noted in the approved authorization. The authorization does not authorize the use of FTI for multiple purposes outside of those noted within the timeframe agreed.

Any agency that receives FTI for an authorized use may not use that information in any manner or for any purpose not consistent with that authorized use.

If an agency needs FTI for a different authorized use under a different provision of IRC § 6103, a separate request must be sent to IRS Disclosure.

The Office of Safeguards validates that an agency's "need and use" of FTI conforms with the governing provisions allowing the disclosure of FTI. The agency's SSR must describe the purpose(s) for which FTI is collected, used, maintained and shared.

IMPORTANT: An ***unauthorized secondary use of FTI is*** specifically ***prohibited*** and may result in discontinuation of disclosures to the agency and imposition of civil or criminal penalties on the responsible officials.



How should FTI data be transferred securely?

The IRS established a ***Secure Data Transfer (SDT)*** program to provide encrypted electronic transmission of FTI between the IRS and trading partners. For support with establishing an IRS SDT account, please submit an SDT Customer Support Request.

Complete information on establishing an SDT account is available in the SDT Handbook. The SDT Handbook is available from a local IRS governmental liaison or a request to the Safeguards mailbox. Only the following types of documents will be accepted via SDT:

- Control File (.txt)
- Adobe (.pdf)
- Word Document (.doc or .docx)
- Excel Document (.xls or.xlsx)
- Zipped File (.zip

NOTE: Contact the **SafeguardReports@irs.gov** mailbox for specific details on how to submit information via SDT.

Are there any State Tax Agency limitations?

FTI may be obtained per IRC § 6103(d) by state tax agencies only to the extent the information is needed for and is reasonably expected to be used for state tax administration.

YES

- An agency's records must include some account of the result of its use of FTI (e.g., disposition of closed cases and summary of revenues generated) or include reasons why the information was not used.
- State tax agencies using FTI to conduct statistical analysis, tax modeling or revenue projections must notify the IRS by submitting a signed Need and Use Justification Statement for Use of Federal Tax Information form and follow the established guidelines (available through the assigned Governmental Liaison).
- Annually, the agency must provide updated information in the SSR regarding its modeling activities that include FTI. In the SSR, the agency must describe:
  - Any use of FTI that is in addition to what was described in the original Need and Use Justification Form
  - Any new, previously unreported internal tax administration compilations that include FTI
  - Changes to the listing of authorized employees (Attachment B to the Need and Use Justification Form)
- If the agency intends to use a contractor or sub-contractor for conducting statistical analysis, tax modeling or revenue projections, it must submit a 45-day notification (see Section 1.9.4, Disclosing FTI to Contractors or Sub-Contractors) prior to contractor or sub-contractor access to the FTI.
- The agency must submit a separate statement detailing the methodology used and data to be used by the contractor or sub-contractor. The Office of Safeguards and Statistics of Income functions will review the information provided to confirm that

NOTE: If any agency continually receives FTI that it is unable to use for any reason, it must contact the IRS official liaison and discuss the need to stop the receipt of this FTI.

How should safeguards be coordinated?

Coordination of safeguards differ from agency to agency due to the diverse purposes require by each individual agency and its divisions- as FTI may be received and used by several quasi-independent units within the agency's organizational structure.

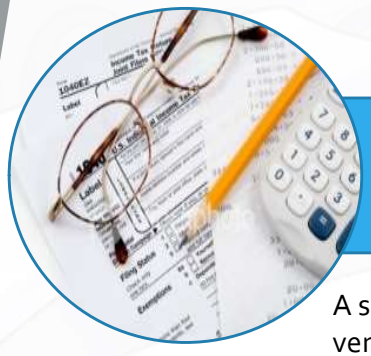
Because of such differences and unique requirements, where there is such a dispersal of FTI, the agency must centralize safeguarding responsibilities to the greatest extent practical and establish and maintain uniform safeguard standards consistent with IRS guidelines. This means that the agency should…

- Identify and assign an official(s) POC that holds a position high enough in the agency's organizational structure to ensure compliance with the agency safeguard standards and procedures.
- Ensure that the selected official(s)/ POC's responsibilities include…
  - Conducts internal inspections;
  - Submits all required safeguard reports to the IRS;
  - Reports Data Breach Incidents Properly and in a timely manner;
  - Develops, Maintains, and Discloses Awareness training; and
  - Serves as a liaison with the IRS.

NOTE: If any agency continually receives FTI that it is unable to use for any reason, it must contact the IRS official liaison and discuss the need to stop the receipt of this FTI.

FTI Safeguards Review

Overview



What are Safeguard Reviews?

A safeguard review is meant to validates the accuracy of the SSR and conformance with the current version of Publication 1075 requirements and The National Institute of Standards and Technology (NIST) Special Publication 800-53.

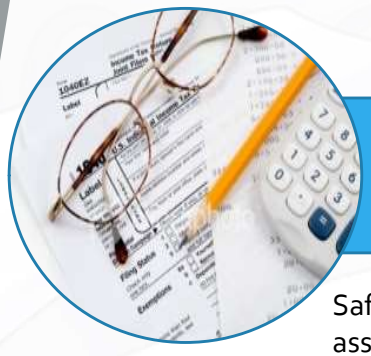
SCOPE

The safeguard review scope will be based on the flow of the FTI, which may include, but is not limited to, field offices, consolidated data centers, off-site storage facilities, disaster recovery sites, contractor and sub-contractor sites.

AGENCY REQUIREMENT

Agencies must facilitate execution of the review methods utilized by Safeguards staff. Agency management approval must be obtained prior to review, if agency policies and procedures contradict any of these methods.

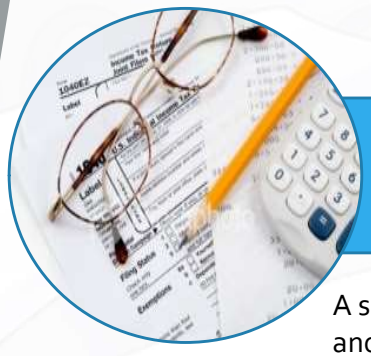
The agency POC will be advised the of critical issues and findings as the review progresses. A briefing will be held with the POC to go over the Preliminary Findings Report (PFR) before the closing conference.



How are Safeguards rated?

Safeguards are assigned a criticality level. The following table provides an overview of the definitions associated with each criticality level use during the process.

Impact Level	Definition
Limited	The potential impact is Limited if the vulnerability could be expected to have a low or minimal adverse effect on the ability to maintain the confidentiality and integrity of FTI.
Moderate	Moderate The potential impact is Moderate if the vulnerability could be expected to have a demonstratable adverse effect on the ability to maintain the confidentiality and integrity of FTI.
Significant	The potential impact is Significant if the vulnerability could be expected to have severe and/or imminent adverse effect on the ability to maintain the confidentiality and integrity of FTI.
Critical	The potential impact is Critical if the vulnerability has an immediate adverse effect on the confidentiality and integrity of FTI.



How are safeguard reviews performed?

A safeguard review is an on-site, remote, or a combination of both (hybrid) evaluation of the use of FTI and the measures employed by the receiving agency and its agents (where authorized) to protect the data.

- **On-site reviews:** Disclosure Enforcement Specialists (DES), Cybersecurity Reviewers (CSR), and Management Officials will conduct an on-site evaluation of the security and privacy controls implemented by the agency and all supporting parties. Assessment techniques include, but are not limited to visual inspections, observations, interviews, document exchange, and automated scanning.
- **Remote reviews:** Disclosure Enforcement Specialists, Cybersecurity Reviewers, and Management Officials will conduct a remote evaluation of the security and privacy controls implemented by the agency and all supporting parties using secured collaborative technologies (e.g., screen-sharing capabilities, teleconferences, video enabled software, etc.). Assessment techniques include, but are not limited to visual inspections, observations, interviews, document exchange, and automated scanning.

This review includes all FTI received whether from the IRS or a secondary source such as SSA, Bureau of the Fiscal Service or another agency (see Federal Tax Information). Safeguard reviews are conducted to determine the adequacy of safeguards as opposed to evaluating an agency's programs. Several factors will be considered when determining the need for a review, the type of review, and the frequency of which a review will be conducted.

Who initiates the safeguard review?

The IRS initiates the review by communication with an agency point of contact (POC) as reported by the agency in the SSR. The preliminary discussion will…

- Be followed by a formal engagement letter to the agency head, which provides official notification of the planned safeguard review. This engagement letter outlines what the review will encompass.
- Include additional requests for specific information that must be provided to the agency POC. These requests may include a list of records to be reviewed (e.g., training manuals, flowcharts, policies, awareness program documentation and organizational charts relating to the processing of FTI).
- Include information prior to the review, in which the agency POC will receive information regarding the manner in which the review will be conducted (e.g., on-site and/or remote), the scope and purpose of the review, a list of the specific areas to be reviewed and agency personnel to be interviewed.

What takes place during the initial review process?

During the review process, A Preliminary Security Evaluation (PSE) call will be held to determine the scope of the review (see NIST Control PM-5 CE-1, Inventory of PII). During this call…

- The electronic flow of FTI will be discussed to provide the review team with a thorough understanding of the location and use of FTI throughout the agency's infrastructure.
- The primary POCs will be introduced, the scope of the review will be defined, assessment logistics will be discussed, and any questions will be answered.

Participants should include agency IT staff knowledgeable about the location and flow of FTI throughout the agency as well as staff or contractors from other locations such as consolidated data centers. As part of the review process, assessors may require…

- Mini-PSE calls for contractors, sub-contractors, off-site locations, etc. in order to obtain additional information to determine the review scope.
- Additional information and clarification to include automated scanning procedures which will be discussed after the PSE call(s) in order to finalize the proposed scope to be provided for review and approval.

What happens during the review?

START

Opening Conference

- Procedures Review
- Data Flow Discussion
- FTI Flow Confirmation
- Review Scope Approval

Operations Observation

- Field Offices
- Consolidated data centers
- Off-Site Storage Facilities
- Disaster Recovery Sites
- Contractor/ Sub-Contractor Sites

Review Methods

- Spot check agency records for FTI
- Employee Interviews
- Facility Tours
- Document Review
- Automated/Manual testing
- Remote Assessment

Agency Involvement

- Must facilitate execution of the review methods utilized by Safeguard staff.
- Agency Management approval must be obtained prior to review, if agency policies and procedures contradict any of the methods identified.

Outcome

- A briefing will be held with the POC to go over the Preliminary Findings Report (PFR) before the closing conference.
- The closing conference is held upon completion of the agency's review, where the PFR is issued to provide the agency an overview of the findings identified during the review.

What happens after the review?

- An SRR and CAP will be issued within 45 days of the closing conference to document the review findings.
- Requests for corrections to the SRR must be emailed to the SafeguardReports@irs.gov mailbox. The Office of Safeguards will respond with an acknowledgement and a determination.
- The Office of Safeguards will identify deadlines for resolution based upon the risk associated with each finding. Outstanding issues must be resolved and addressed in the next reporting cycle of the CAP.
- If the Agency has any critical findings, the agency must submit a mitigation plan to Safeguards within 7 days from the closing conference date. Safeguards will report the critical findings along with your agency plan to the Treasury Inspector General for Tax Administration (TIGTA).
- The CAP must be updated and submitted semi-annually using the last CAP issued by the Office of Safeguards (see Section 2.E.5, Corrective Action Plan) until all review findings are accepted as closed.
- If an agency has a CAP due within 60 days of the review, that CAP is not required because the remaining open findings will be handled as part of the upcoming on-site or remote Safeguard Review Each CAP submission must include an explanation and/or evidence of actions already taken or planned to resolve all outstanding findings.
- The agency must submit an actual or planned implementation date for each outstanding finding.

Termination of FTI Use Requirements

Overview

What steps should the agency take when FTI is no longer required?

Notify the IRS Safeguard Team

- Send e-mail to SafeguardReports@irs.gov
- Include the following:
  - Copies of notifications to all agencies from which FTI is received, that FTI will no longer be requested.
  - Letter from the Head of Agency certifying that all residual FTI has been destroyed in accordance with IRC Disposal Requirements. (See Section 2.F Disposal of FTI – IRC § 6103(p)(4)(F))

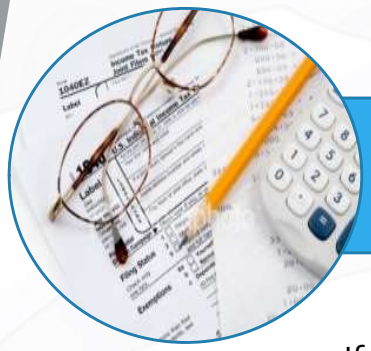
Once documentation is reviewed, the Office of Safeguards will send an acknowledgement of the agency's termination, instructions on Safeguard reporting and on-site review obligations. Instructions for reinstatement will be included in the acknowledgement letter.

How should agencies archive FTI?

NOTE: This section is for agencies terminating receipt of FTI but required by statute to retain FTI for designated periods.

If residual FTI is required to be retained by statute for a designated period (e.g., 5 or 10 years), then agencies must:

- Ensure that a currently authorized agency, contractors, or sub-contractor retain FTI in accordance with Publication 1075 security standards
- Provide copies of notifications as shown in Section 1.7.1.1, Termination Documentation
- Submit an annual SSR each year while the agency has possession or oversight of the data
- Continue to be subject to periodic Safeguard Reviews
- Submit a letter from Head of Agency certifying that all residual FTI has been destroyed when the retention period has ended



What happens if IRS Suspends, Terminates or puts an Agency under Administration Review?

If the IRS terminates the transmission of FTI, the agency will notify the authorized POC in writing and may suspend further disclosures **IF** it is deemed that the Federal Tax Administration can be seriously impaired.

The IRS may terminate or suspend disclosure of return and return information to any authorized recipient under 6103(p)(4), if the IRS determines that :

1. The authorized recipient (or agency) has allowed an unauthorized inspection or disclosure of FTI and has not taken adequate corrective action to prevent the recurrence of an unauthorized inspection or disclosure; or
2. 2. The authorized recipient does not satisfactorily maintain the safeguards prescribed by Section 6103(p)(4) and Publication 1075 and has made no adequate plan to improve its system to maintain the safeguards satisfactorily.

Agencies in receipt of the termination or suspension letter may appeal the determination as outlined in Exhibit 3, USC Title 26, CFR § 301.6103(p)(7)-1 **(Pg. 194)**

Reporting Improper Inspections or Disclosures

Overview

What is a DATA INCIDENT and how should the agency handle it?

A ***data incident*** is an occurrence that…

1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality or availability of information or an information system; or
2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures or acceptable use policies. Incidental and inadvertent accesses are considered data incidents.

An incident involving the loss or theft of an IRS asset containing FTI, or the loss or theft of a physical document that includes FTI, or the inadvertent disclosure of FTI, is known as a data breach. ***[See next slide]***

Often, an occurrence may be first identified as an incident, but later identified as a data breach once it is determined that the incident involves FTI. This is often the case with a lost or stolen laptop or electronic storage device.

Information spillage refers to instances where FTI is inadvertently placed on systems that are not authorized to handle FTI or are not part of the agency's intended FTI workflow. Upon discovery, corrective action is required to remove the FTI from the unintended system and ensure there were no unauthorized accesses or disclosures. If no FTI is involved, then there is no need to report the spill to the Office of Safeguards or TIGTA. If the agency cannot show FTI was not involved within that 24-hour period, then the spill will need to be reported to the Office of Safeguards and TIGTA.

What is a DATA BREACH and how should the agency handle it?

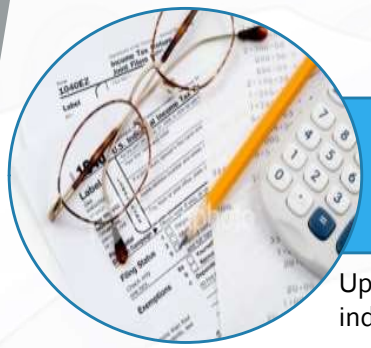
A data breach is a type of incident involving a loss, theft, or inadvertent disclosure of FTI. A data breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

- A person other than an authorized user accesses or potentially accesses FTI or,
- An authorized user accesses or potentially accesses FTI for an unauthorized purpose.

A data breach is not limited to an occurrence where a person other than an authorized user potentially accesses FTI by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A data breach may also include the loss or theft of physical documents that include FTI and portable electronic storage media that store FTI, the inadvertent disclosure of FTI on a public website or an oral disclosure of FTI to a person who is not authorized to receive that information. It may also include an authorized user accessing FTI for an unauthorized purpose.

Some common examples of a data breach include:

- A laptop or portable storage device storing FTI is lost or stolen.
- An email containing FTI is inadvertently sent to the wrong person.
- A box of documents with FTI is lost or stolen during shipping.
- An unauthorized third party overhears agency employees discussing FTI.
- A user with authorized access to FTI sells it for personal gain or disseminates it.
- An IT system that maintains FTI is accessed by a malicious actor.
- FTI is posted inadvertently on a public website.



Who should the agency notify in the event of a data breach and how?

Upon discovery of a possible improper inspection or disclosure of FTI, including breaches and incidents- the individual making the observation or receiving information must contact…

- The Treasury Inspector General for Tax Administration (TIGTA) Field Division office, to the Special Agent-in-Charge, immediately, but no later than 24 hours after identification of a possible issue involving FTI. See NIST IR-6, Incident Reporting and IR-8, Incident Response Plan. The Local TIGTA Field Division Office contact information can be found on the TIGTA website at https://www.treasury.gov/tigta/oi_office.shtml.
- Concurrent to notifying TIGTA, the agency must notify the Office of Safeguards by email to Safeguards mailbox, safeguardreports@irs.gov . **[See next slide for details on what MUST be included]**

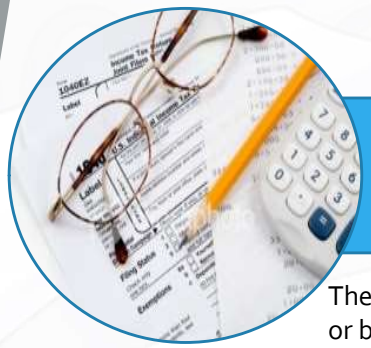
If unable to contact the local TIGTA Field Division, contact the Hotline Number.

- **Hotline Number:** 800-366-4484 **during normal working hours** for immediate assistance.

> **Note: After regular business hours,** call ***800-589-3718***. This number reaches an answering service which answers all calls from all locations in the United States 24 hours a day 7 days a week. The answering service will contact the on-call TIGTA agent. TIGTA Homepage: https://www.treasury.gov/tigta

- **Mailing Address**:
  - Treasury Inspector General for Tax Administration Ben Franklin Station P.O. Box 589 Washington, DC 20044-0589

For intrusions, manipulations or compromises of computer networks, as well as external cyber-based actions that interfere with the IRS's ability to conduct electronic tax administration, or any breach that involves unauthorized disclosure within an IT environment, contact ***TIGTA Electronic Crimes & Intelligence Division*** at cybercrimes@tigta.treas.gov .



What should the agency include in the notification to the Safeguard Team?

The email notification to be submitted to the Safeguard Team must include the agency's specifics of the incident or breach known at that time into a data incident report, including but not limited to:

- Name of agency and agency POC for resolving data incident with contact information
- Date and time the incident/breach occurred
- Date and time the incident/breach was discovered
- How the incident/breach was discovered
- Description of the incident/breach and the data involved, including specific data elements, if known
- Potential number of FTI records involved; if unknown, provide a range if possible
- Address where the incident/breach occurred
- IT involved (e.g., laptop, server, mainframe)
- Does the incident involve an unauthorized access or disclosure by an agency employee? (Y/N)
- If a criminal indictment is not pursued, will a disciplinary or adverse action be proposed against the agency employee involved in this unauthorized access or disclosure? (Y/N)

The Reports should be sent to:

- Safeguards mailbox, safeguardreports@irs.gov. Use the term "data incident report" in the subject line of the email. Do not include any FTI in the data incident report.
- Reports must be sent electronically and encrypted via IRS-approved encryption techniques as outlined in ***Section 2.E.3, Encryption Requirements***. ***[pg. 67]***

NOTE: Even if all information is not available, immediate notification is the most important factor, not the completeness of the data incident report. Additional information must be provided to the Office of Safeguards as soon as it is available. The agency will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.

What should the Response Procedures and Response incorporate?

The procedures must follow the National Institute of Standards and Technology (NIST) Incident Response Control requirements. During an active incident, the agency should take a closer look at the following controls in a more granular level and document any deficiencies that must be addressed ASAP as part of the response.

IR-1 Incident Response Policy and Procedures

IR-4 Incident Handling

IR-5 Incident Monitoring

Upon discovery of an incident or data breach, the agency must…

Contact TIGTA and IRS immediately or within 24 hours of breach or disclosure discovery.
DO NOT WAIT TO CONDUCT AN INTERNAL INVESTIGATION TO DETERMINE IF FTI WAS INVOLVED.

Ensure that NIST ***Control IR-1 > Incident Response Policy and Procedures*** is used when responding.

Safeguard Team Response

- The team will coordinate with the agency regarding the appropriate follow-up actions required to be taken by the agency to ensure continued protection of FTI.

What must the agency do when notifying the impacted individuals?

The agency must provide a written notification to a taxpayer whose FTI was subject to unauthorized access or disclosure when a disciplinary or adverse action is proposed against the agency employee responsible. The required written notification to the taxpayer must include the date of the unauthorized inspection or disclosure and the rights of the taxpayer under IRC § 7431.

The agency must confirm to the Office of Safeguards when the required written notification to the taxpayer is completed. In addition, the agency must inform the Office of Safeguards of any pending media releases, including sharing a draft of the release, prior to distribution.

What steps must the agency take post-incident?

The agency should review the following controls:

IR-1 Incident Response Policy and Procedures . Conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance. Any deciciencies identified within must be resolved ASAP.

AT-3 Role Base Training– Conduct a post incident review of the Incident's Response Training Modules addressing handling response and re-train all employees, contractors, sub-contractors, and data center personnel.

IR-4 Incident Handling – Update and document results associated with the incident handling response and test the response capabilities annually using table exercises to determine its effectiveness.

IR-5 Incident Monitoring - Track and document all system security and privacy incidents.

Disclosure of FTI To Others

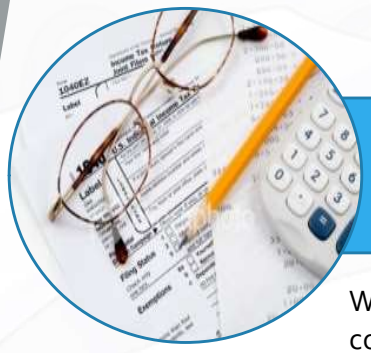
Overview

Can FTI Data be shared with others?

Disclosure of FTI is prohibited unless authorized by statute. Agencies with access to FTI are not allowed to make further disclosures of that information to their agents, contractor, or sub-contractor unless authorized by statute. See ***NIST Control AC-21, Information Sharing***.

Agencies must use specific language in their contractual agreements that clearly state the requirements necessary to protect the confidentiality of FTI and avoid ambivalence or ambiguity (see the model language of Exhibit 7). For additional requirements on contracts, see Exhibit 6, Contractor 45-Day Notification Procedures. **[pg. 200]**

Absent specific language in the IRC or where the IRC is silent in authorizing an agency to make further disclosures, the IRS's position is that further disclosures are unauthorized.



What precautions should an agency take when disclosures are authorized?

When disclosure of FTI is authorized, the agency must take certain precautions prior to redisclosure to a contractor or sub-contractor, namely:

- Has the IRS been given sufficient notice prior to releasing FTI to a contractor or sub-contractor?
- Has the agency been given reasonable assurance through a visitation or received a report certifying that all security standards (physical and IT systems) have been addressed?
- Does the contract authorizing the disclosure of FTI have the appropriate safeguard language? See the model language of ***Exhibit 7, Safeguarding Contract Language***.

Agencies MUST…

- Fully report to the IRS in their SSRs all disclosures of FTI to contractors and subcontractors. Any additional disclosures to contractors and sub-contractors must be reported using the Notification process and reported on the next annual SSR.

Agencies MUST NOT…

- Contract for the disclosure of FTI that is not authorized by IRC § 6103. Only contracts for services that require access to FTI to perform their duties under the contract are required to comply with these standards.

What precautions should an agency take when dealing with External Provider?

An external provider refers to organizations other than the agency operating or acquiring the system. External providers include, but is not limited to …

- contractors or sub-contractors; and
- other organizations providing system development, information technology services, outsourced applications, testing/assessment services and network and security management.

Agencies must include personnel security requirements in contracts. External providers may have personnel working at agency facilities with credentials, badges or system privileges. Notifications of external personnel changes ensure appropriate termination of privileges and credentials. See ***NIST Control PS-7, External Personnel Security.***

What steps should the agency take prior to Disclosing FTI to Contractors or Sub-Contractors?

There are 10 key items The agency MUST DO and they are…

If the agency requires the use of a contractor to conduct ***tax modeling, revenue estimation or other statistical activities, 45-day notification requirements apply*** (see Section 1.9.4, Disclosing FTI to Contractors or PP Slide 40).

01 Notify the Office of Safeguards prior to re-disclosing FTI to contractors or sub-contractors,

02 Notify and obtain written approval from the Office of Safeguards prior to re-disclosing FTI to sub-contractors (when the agency's contractor uses or desires to re-disclose FTI to another contractor)

03 Establish privacy roles and responsibilities for contractors or sub-contractors and service providers to safeguard the confidentiality and integrity of FTI.

04 Include privacy requirements in contracts and other acquisition-related documents and require that contractors, sub-contractors, or other agents have requirements in effect to provide safeguards required under IRC § 6103(p)(4) to protect FTI

05 Where appropriate, enter into a contract, an SLA, memoranda of understanding, memoranda of agreement, letters of intent, computer matching agreement or similar agreement, with third parties that specifically describe the FTI covered and specifically enumerate the purposes for which the FTI may be used.

What steps should the agency take prior to Disclosing FTI to Contractors or Sub-Contractors?

(Cont.) > The agency MUST…

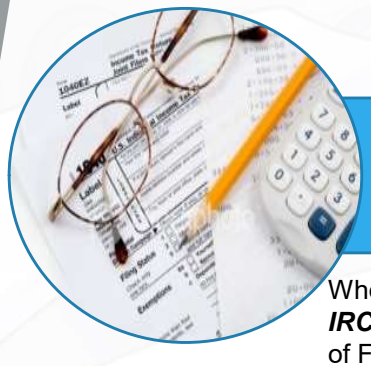
06 Share FTI externally only for the purposes statutorily authorized and provide the Office of Safeguards with an annual certification that each contractor, sub- contractor, or other agent is in compliance with the requirements noted as part of the report required under IRC § 6103(p)(4)(E).

07 Monitor, audit and train its staff on the authorized uses and sharing of FTI with third parties and on the consequences of unauthorized use or sharing of FTI by conducting on-site reviews of contractors, sub-contractors, and other agents and provide the findings of these reviews to Safeguards as part of the report required under IRC § 6103(p)(4)(E).

08 Require agency notification of contractor or sub-contractor personnel changes to ensure appropriate termination of privileges and credentials. See NIST Control PS-7, External Personnel Security.

09 Evaluate any proposed new instances of sharing FTI with third parties to assess whether they are authorized.

10 Require contractor or sub-contractor employ a formal sanction process for contractor employees and, when permitted by statute, sub-contractor employees failing to comply with established information security policies and procedures for FTI. Notification of designated agency personnel is required within 72 hours.



What steps should the agency take when handling re-disclosure of FTI to another entity?

When required regulatory prerequisite steps are satisfied and where appropriate***, under the authority of IRC § 6103(p)(2)(B***), the IRS may execute an agreement with an agency that authorizes the re-disclosure of FTI to another entity. These agreements are negotiated and approved by IRS Disclosure with concurrence of the Office of Safeguards.

Federal agencies authorized by statute to enter into re-disclosure agreements are ***required to provide a list of all executed agreements annually in the SSR.*** Agreements must include language to enforce the requirements for:

- Incident reporting related to FTI
- Implementing personnel sanctions for failure to comply with established information security policy and procedures related to FTI
- Confirmation to the agency any proposals of disciplinary and adverse action concerning unauthorized accesses and disclosures involving FTI
- Notification of individuals whose FTI was subject to unauthorized access or disclosure including the date the unauthorized access or disclosure of FTI occurred.

When requested by the Office of Safeguards, agencies must ***provide a copy of all re-disclosure agreements within 30 days.*** An electronic copy must be sent to the Office of Safeguards via SDT. If SDT is not available, the agreements may be emailed to the SafeguardReports@irs.gov mailbox

Return Information in Statistical Reports

Overview

Can FTI data be used for statistical reports and/or tax administration purposes?

IRC § 6103 authorizes the disclosure of FTI to specific federal agencies for use in statistical reports, tax administration purposes and certain other purposes specified in IRC § 6103(j). Statistical reports may only be released in a form that cannot be associated with, or otherwise identify, directly or indirectly, a particular taxpayer.

Agencies authorized to produce statistical reports must adhere to the following guidelines or an equivalent alternative that has been approved by the IRS:

- Access to FTI must be restricted to authorized personnel.
- No statistical tabulation may be released outside the agency with cells containing data from fewer than three returns. The exception to this rule is for corporation returns where no tabulation with cells containing data for fewer than five returns may be released.
- Statistical tabulations prepared at the state level may not be released for cells containing data for fewer than 10 returns. Data for geographic areas below the state level such as county may not be released with cells containing data from fewer than 20 returns. In addition, for tabular data at the ZIP Code level, additional procedures must be employed. Individual ZIP Code areas with fewer than 100 returns cannot be shown. Additionally, any cell in the ZIP Code table based on fewer than 20 returns cannot be shown. Finally, individual returns that represent a large percentage of the total of a particular cell must be excluded from the data.
- Tabulations that would pertain to specifically identified taxpayers or that would tend to identify a particular taxpayer, either directly or indirectly, may not be released.

YES

Federal agencies seeking statistical information from the IRS must make their requests under IRC § 6103(j). The requests must be addressed to:

Director, Statistics of Income Division
Internal Revenue Service, OS:P:S
1111 Constitution Avenue, NW
Washington, D.C. 20224

Can State Tax Agencies leverage FTI data for statistical purposes?

YES

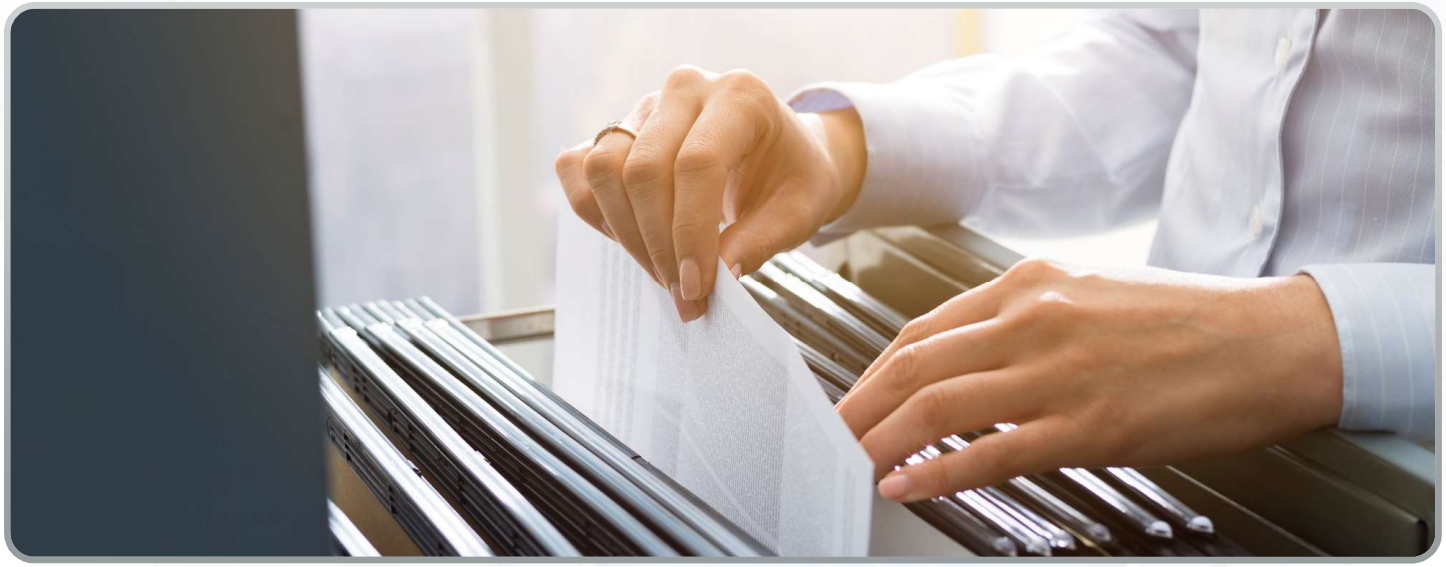
State tax agencies must provide written notification and obtain IRS approval prior to performing tax modeling, revenue estimation or other statistical activities involving FTI. The agency must demonstrate that the activity is required for tax administration purposes. The agency must adhere to the following process to submit a request:

1) Contact the local IRS disclosure manager2 and complete a Need and Use Justification for Federal Tax Information Form.
2) The completed and signed form must be returned to the IRS disclosure manager for review and approval. The Office of Safeguards will be notified by the IRS disclosure manager of the request and approval.
3) Changes to the terms of the statistical analysis activities documented in the form must be submitted to the IRS Office of Safeguards as part of the annual SSR (see Section 1.4, State Tax Agency Limitations and Section 2.E.4, Safeguard Security Report).
4) Updates to the form must be made as requested by the IRS disclosure manager.

If the agency requires the use of a contractor to conduct tax modeling, revenue estimation or other statistical activities, a 45-day notification requirement applies

Physical Security Requirements

Overview



FTI Data Recordkeeping > IRC § 6103(p)(4)(A)

Internal and External Requirements Overview

What are the GENERAL Record Keeping Requirements?

Federal, state and local agencies, bodies, commissions and agents authorized under IRC § 6103 to receive FTI are ***required by IRC § 6103(p)(4)(A)*** **to establish a permanent system of standardized records of requests made by or to them for disclosure of FTI**. For additional guidance, see Exhibit 2, USC Title 26, IRC § 6103(p)(4).

This recordkeeping mechanisms are required to track the movement of FTI and must…

- **Include internal requests among agency employees as well as requests outside of the agency.**
- **Be maintained for a minimum of five (5) years.**

NOTE: The Safeguards website contains guidance, job aids, helpful tools and frequently asked questions to assist agencies in meeting safeguard requirements; see http://www.irs.gov/uac/Safeguards-Program .

What should FTI Logs include? [Electronic and non-electronic]

The agency must establish a tracking system to identify and track the location of electronic and non-electronic FTI from receipt until it is destroyed. The FTI log may include, but is not limited to, the following tracking elements:

Taxpayer Identifier *	Type of Information (e.g., revenue agent reports, Form 1040, work papers)
Tax year(s)	Date Received
Date Requested and Reason for Request	Exact Location of FTI
Details on WHO has had access to FTI Data	If disposed, date and method of disposition

If the authority to make further disclosures is present (e.g., agents/contractors/sub-contractors), information disclosed outside the agency must be recorded on a separate list or log. The log must:

Reflect to whom the disclosure was made	Why it was disclosed
What was disclosed	When it was disclosed

NOTE: *To the extent possible, do not include FTI in the log. If FTI is used, the log must be secured in accordance with all other safeguarding requirements.

What should FTI Logs include? (Cont.) [Electronic and non-electronic]

Agencies transmitting FTI from one mainframe computer to another, as in the case of the SSA sending FTI to state human services agencies, need only identify the bulk records transmitted. This identification will contain …

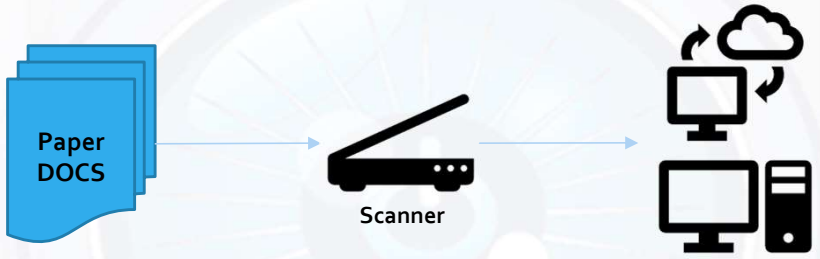
- The approximate number of taxpayer records
- The best possible description of the records
- The date of the transmissions
- The name of the individual making/receiving the transmission

Figure 1 – Sample FTI Logs

FTI Log									
Date Requested	Date Received	Taxpayer Identifier	Tax Year(s)	Type of Information	Reason for Request	Exact Location	Who has access?	Disposition Date	Disposition Method

FTI Bulk Transfer Log								
Date Received	Control Number/File Name	Content (do not include FTI)	Recipient/Title Location	Number of Records	Movement Date	Recipient/Title Location	Disposition Date	Disposition Method

How should FTI Data conversion from paper to media be handled?



Conversion of FTI from paper to electronic media (scanning) or from electronic media to paper (print screens or printed reports) must…

- Be tracked from creation to destruction of converted FTI.
- Include the log fields detailed in the previous slides [45 & 46].

What type of recordkeeping should agencies enforce when disclosing FTI to State Auditors?

***When disclosures are made by a state tax agency to state auditors*, recordkeeping requirements pertain only in instances where the auditors use FTI for further scrutiny and inclusion in their work papers**.

***In instances where auditors read large volumes of records containing FTI, whether in paper or electronic format*, the state tax agency need only identify bulk records examined**. This identification must include…

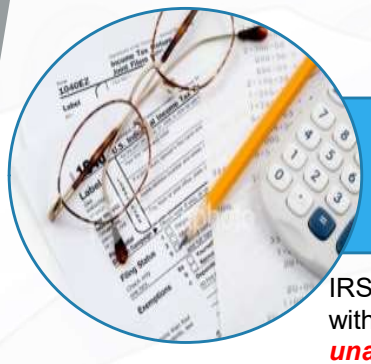
- **The approximate number of taxpayer records**
- **A description of the records**
- **The date of inspection**
- **The name of the individual(s) making the inspection**

Recordkeeping log samples are provided in ***Slide 47***

IMPORTANT: Disclosure of FTI to auditors external to child support enforcement, human services or labor benefit agencies is not authorized by statute. FTI in case files must be removed prior to access by the auditors.

Secure Storage > IRC § 6103(p)(4)(B)

Physical Security Requirements Overview



What are the minimum requirements to enforce Secure Storage?

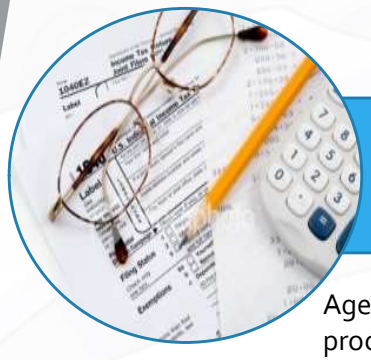
IRS has established a Minimum Protection Standards (MPS) guideline that is designed to provide management with a basic framework of minimum-security requirements. ***The objective*** of these ***standards is to prevent unauthorized access to FTI***. **MPS thus requires two barriers**. Example barriers under the concept of MPS are outlined in the following table:

Secured Perimeter	The perimeter is enclosed by slab-to-slab walls constructed of durable materials and supplemented by periodic inspection. Any lesser-type partition must be supplemented by electronic intrusion detection and fire detection systems. All doors entering the space must be locked in accordance with Locking Systems for Secured Areas. In the case of a fence/gate, the fence must have intrusion detection devices or be continually guarded, and the gate must be either guarded or locked with intrusion alarms.
Security Room	A security room is a room that has been constructed to resist forced entry. The entire room must be enclosed by slab-to-slab walls constructed of approved materials (e.g., masonry brick, concrete) and supplemented by periodic inspection and entrance must be limited to specifically authorized personnel. Door hinge pins must be non-removable or installed on the inside of the room.
Badged Employee	During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear picture identification badges or credentials. The badge must be clearly displayed and worn above the waist.
Security Container	A security container is a storage device (e.g., turtle case, safe/vault, locked IT cabinet) with a resistance to forced penetration, and a security lock with controlled access to keys or combinations.

The MPS or "two-barrier" rule applies to FTI, beginning at the FTI itself and extending outward to individuals without a need-to-know.

MPS provides the capability to deter, delay or detect surreptitious entry. Protected information must be containerized in areas where unauthorized employees may have access after-hours.

IMPORTANT: The applicability of this requirements is on a case-by-case basis due to local factors which may require additional security measures. Therefore, management must analyze local circumstances to determine location, container, and other physical security needs at individual facilities.



What items should be stored securely and how?

Agencies must ensure that anything use to gather, store, transmit or process FTI data such as…

- Paper Document
- Multi-function Devices
- Physical Workspace
- Workstations/ Servers

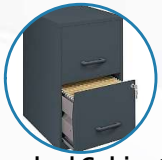
Must incorporate a minimum of two physical security measures, which includes but is not limited to, the following mechanism:


Vault


Locked Room


Secured Building


Secured Access


Locked Cabinet

Security Guards


Secured Fence


Secured Perimeter

Multifunction Devices (MFDs) or High-Volume Printers, Scanners and/or Fax Machines must be locked with a mechanism to prevent physical access to the hard disk/memory or meet MPS.

For additional guidance, see ***NIST Control PE-3, Physical Access Control***.

The IRS has categorized federal tax information as moderate risk. The minimum protection standards (MPS) must be used as an aid in determining the method of safeguarding FTI. These controls are intended to protect FTI in paper and electronic form.

NOTE: How the required security is provided depends on the facility, the function of the activity, how the activity is organized and what equipment is available. Proper planning and organization will enhance the security while balancing the costs.

What steps should be taken to Restricted Area Access ?

Care must be taken to deny unauthorized access to areas containing FTI during duty and non-duty hours.

This can be accomplished by creating…

Restricted Areas | **Security Rooms** | **Locked Rooms**

Additionally, FTI in any form (computer printout, photocopies, tapes, notes) must be protected during non-duty hours. This can be done through a combination that includes a combination of various mechanisms …

Secured Perimeter | **Secured Container** | **Secured Building**

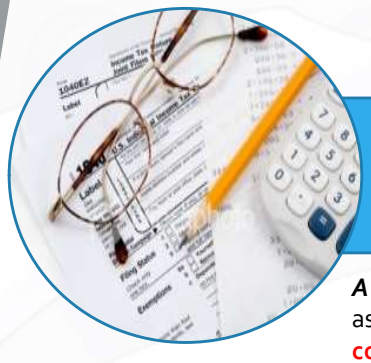
A restricted area is an area where entry is limited to authorized personnel (individuals assigned to the area). ***Using restricted areas is an effective method for eliminating unnecessary traffic through critical areas, thereby reducing the opportunity for unauthorized access, disclosure, or theft of FTI.*** **To qualify as a restrictive area, ALL of the following items must be in place…**

- Restricted areas MJST be separated from non-restricted areas by physical barriers that control access.
- The number of entrances MUST be kept to a minimum and must have controlled access (e.g., electronic access control, key access, door monitor) to prevent unauthorized entry.
- The main entrance MUST be controlled by locating the desk of a responsible employee at the entrance to ensure that only authorized personnel with an official need may enter.

How should Access to spaces containing FTI Data be secured?

The agency must…

- Maintain an authorized list of all personnel who have access to information system areas, where these systems contain FTI. **NOTE:** This does not apply to those areas within the facility officially designated as publicly accessible
- Maintain a policy addressing issuance of appropriate authorization credentials, including badges, identification cards or smart cards. **NOTE:** This policy must include proper use and accountability requirements.
- Maintain a list that identifies those individuals who have authorized access to any systems where FTI is housed. **NOTE:** Access authorizations and records maintained in electronic form are acceptable.
- Control physical access to the information system devices that display FTI information or where FTI is processed to prevent unauthorized individuals from observing the display output. For additional information, see ***NIST Control PE-5, Access Control for Output Devices.***
- Monitor physical access to the information system where FTI is stored to detect and respond to physical security incidents. For additional information, see ***NIST Control PE-6, Monitoring Physical Access***
- Position information system components within the facility to minimize the opportunity for unauthorized access.
- Always make sure than an authorized employee is present whenever cleaning and facility maintenance personnel work in restricted areas containing unsecured FTI.
- Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.
- Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations and if not, then the agency must designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities. ***See NIST MA-5, Maintenance Personnel***.
- Ensure that the organizations Policy and Policy Training Modules include the prohibition of personnel allowing an individual to "piggyback" or "tailgate" into restricted locations.
- Ensure that all individuals entering an area containing FTI do not bypass access controls or allow unauthorized entry of other individuals. Unauthorized access must be challenged by authorized individuals (e.g., those with access to FTI). Security personnel must be notified of piggyback/tailgate attempts.



When and Where should Visitor Access Logs be maintained?

A visitor access log must be maintained at a designated entrance to a restricted area and all visitors (persons not assigned to the area) ***entering the area shall be directed to the designated entrance***. **Prior to accessing areas that contain FTI, a visitor must sign a visitor access log.**

The security personnel, if any, MUST…

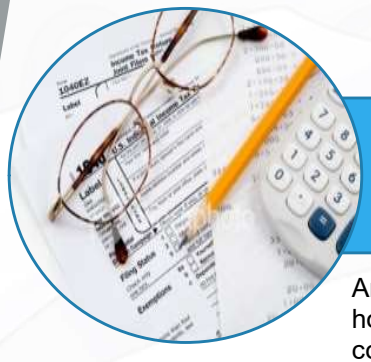
- validate the person's identity by examining government-issued identification (e.g., state driver's license or passport).
- compare the name and signature entered in the access log with the name and signature of the government-issued identification.
- When leaving the area, the security personnel or escort must enter the visitor's time of departure into the log.

The ***visitor access log*** must require the visitor to provide the following information:

Name and Organization of Visitor	**Time of entry and departure**	**Form of Identification**	**Purpose of visit**
Date of Access	**Signature of visitor**	**Name and organization of person visited**	

Visitor Access Log							
Date	Name & Org of Visitor	Form of Visitor ID	Purpose of Visit	Name & Org of Person Visited	Time of Entry	Time of Departure	Signature of Visitor

IMPORTANT: **Each restricted area access log must be closed out at the end of each month and reviewed by management. Visitor access logs must be retained for five (5) years**



What is an Authorized Access List and what should it include?

An Authorized Access List keeps track of everyone who has access to the facilities to which FTI Data may be hosted. It facilitates the entry of employees/vendor/contractor/non-agency personnel who have a frequent and continuing need to enter a restricted area, but who are not assigned to the area, an Authorized Access List (AAL) can be maintained so long as MPS are enforced.

The AAL must contain the following:

- Name of employee/vendor/contractor/non-agency personnel
- Agency or department name
- Name and phone number of the agency POC authorizing access
- Address of agency/vendor/contractor
- Purpose and level of access

If there is any doubt of the identity of the individual, the security monitor must verify the identity of the individual against the AAL prior to allowing entry into the restricted area.

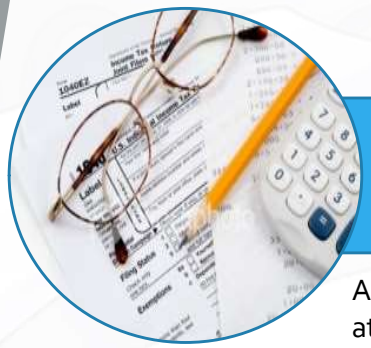
For additional guidance, see ***NIST Control PE-2, Physical Access Authorizations***. Also, see ***NIST Control PE-16***, Delivery and Removal, for guidance on controlling information system components entering and exiting the restricted area.

IMPORTANT: AAL must be reviewed monthly or upon occurrence or potential indication of an event such as a possible security breach or personnel change.

How should enforcement of Safeguarding Keys and Combinations be applied?

Agencies must ensure that…

- All containers, rooms, buildings, and facilities containing FTI are locked when not in actual use.
- Access to a locked area, room or container can be controlled only when the key or combination is controlled. Compromising a combination or losing a key negates the security provided by that lock. Combinations to locks must…
  - Be changed annually or when an employee who knows the combination retires, terminates employment or transfers to another position.
  - Combinations are given only to those who have a need to have access to the area, room or container and must never be written on a sticky-note, calendar pad or any other item (even though it is carried on one's person or hidden from view).
  - An envelope containing the combination are secured using the same security measures for the envelope as the locked material.
- Access control measures (keys, proximity cards, combinations) are issued only to individuals having a need to access an area, room, or container.
- Inventory records are maintained and must account for the total number of keys, proximity cards, combinations, etc. that are available and issued. The inventory must account for master keys and key duplicates. An annual reconciliation must be done on all key records.
- The number of keys or persons with knowledge of the combination to a secured area must be kept to a minimum. Keys and combinations will be given only to those individuals who have a frequent need to access the area.



What mechanisms can be implemented to limit access to secure environments?

Agencies should leverage access control mechanisms that provide the capability to audit access control attempts and that can be configured to keep track of access control logs addressing successful and failed attempts to secured areas containing FTI or systems that process FTI. This mechanisms include but are not limited to:

Badge Reader

Smart PIV Card

Biometrics

Agency personnel must review access control logs on a monthly basis. The access control log must contain the following elements:

- Owner of the access control device requesting access
- Success/failure of the request
- Date and time of the request

FTI in Transit

Requirements Overview

How should FTI Data be handled while in Transit?

Agencies must ensure that FTI does not become misplaced or available to unauthorized personnel while it is transported from one location to another. Therefore, when FTI is hand-carried by an individual in connection with a trip or in the course of daily activities, the information must be kept with that individual and protected from unauthorized disclosures as follow:

- **Records in transit must be fully documented using a transmittal form.**
- **Records send via courier/messenger service must be double-sealed and the internal envelope must be marked confidential.**
- **The transmittal form must document the shipment, the time it was received, and acknowledged by the receiving party. .**
- **The internal package must include a confidential statement denoting that only the designated official or delegate is authorized to open it.**
- **Compact Disk (CD), digital video disks (DVD), thumb drives, hard drives, tapes and microforms MUST, when feasible, be fully encrypted using AES 256+**
- **The external package MUST NOT be labeled as FTI or include any indication that the content contains FTI.**

NOTE: Encryption requirement added to guidance as part of NIST 800-53 controls requirements.

How should FTI Data be handled During Office Moves?

Agencies must make plans to protect and account for all FTI properly. This means that the means to move FTI Data properly must include any of the following mechanisms while in transit:

Locked Vault/Box

Locked Cabinet

Envelop inside Envelop (internal envelop sealed

Sealed Box with tampering protection

In addition to the mechanisms noted above, FTI MUST remain in the custody of an Agency employee for whom accountability is tracked and maintained to ensure that the package, cabinets, or boxes don't become misplaced or lost during the move. In addition, digital media must…

- Be in a secure area with restricted access.
- Enforce FULL DISK Encryption when restricted access isn't viable.
- Enforce File Level Encryption in all mobile devices when supported.
- Be kept in a secured area under the immediate protection and control of an authorized employee.
- Locked properly when not in use or in the care of an authorized employee.
- Fully inventoried, maintained, and review semi-annually for control and accountability.

How should FTI Data be handled In an Off-Site Storage Facility?

Agencies MUST ensure that any media containing FTI DATA is properly secured, labeled, and protected from unauthorized individuals. Therefore, it is essential for the agencies to ensure that contractor-operated off-site storage facilities that comply with ALL Safeguarding Requirements..

- Visitor Access Log
- Access Restrictions
- Internal Inspections
- Employee Training

NOTE: This requirements MUST be fully included within the contract agreement and understand that they are subject to IRS Safeguards reviews. See Exhibit 7: Safeguarding Contract Language

Airtight Turtle Case

Agencies without the statutory authority to contract for services involving the disclosure of FTI (e.g., state Human Services and certain workforce agencies not receiving data under 6103(d)), may NOT allow the release of media containing FTI to a contractor-operated off-site storage facility unless the following conditions are met:

- The media is encrypted and labeled as containing "FEDERAL TAX INFORMATION".
- The media is LOCKED in a turtle case or security container.
- The agency retains the key to the turtle case

How about an Alternate Work Site?

If the confidentiality of FTI can be adequately protected, telework such as employee's homes or other non-traditional work sites can be use; however, the safeguard requirements do not change, and training will be essential to ensure FTI data is protected properly.

How should the equipment and digital storage handling FTI be secured in alternate sites?

Agencies MUST retain FULL Ownership and control for all hardware, software, and end-point equipment connecting to public communication networks, including alternate work sites. If non-agency-owned devices are used, a virtual desktop infrastructure is an acceptable alternative when the requirements noted in Section 3.3.7 Virtual Desktop Infrastructure is met. In addition, when employees are allowed to leverage an alternate location, agencies must ensure that…

- They have a specific room or area with appropriate space.
- They have a way to communicate with Management or other members of the agency if security problems arise.
- They have access to locking file cabinets or desk drawers to secure documents, disks, and tax returns when not in use. If agency doesn't provide furniture, it must ensure that adequate means of storage exist at the alternate site.
- The agency provides "locking hardware" to secure automated data processing equipment to large objects, such as desks or tables.

Virtual Desktop

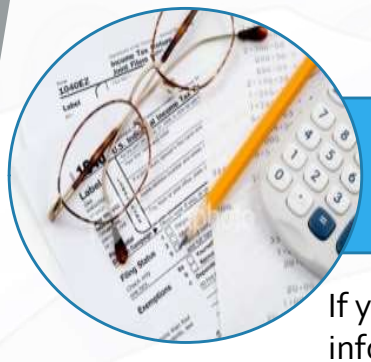
What about storing data- what security measures should be applied?

Agencies MUST ensure that FTI is stored on hard disks IF agency-approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance including upgrades and are being used. Access controls must include…

- Password Security
- Audit Trail
- Encryption
- Virus Detection
- Data Overwriting

FTI Requirements

Overview



Handling of a PHISHING E-Mail

If you receive an **email** claiming to be from the IRS that contains a request for personal information, taxes associated with a large investment, inheritance or lottery.

Don't Reply.
Don't Open Attachments.
Don't Click any links.

Forward any e-mail claiming to be from IRS with full headers as-is to phishing@irs.gov **(No scan images)**

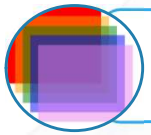
Delete the e-mail and associated attachments once forwarded to IRS. (Validate it was SENT prior to action)

If you clicked a link and entered confidential information, visit https://www.irs.gov/identity-theft-fraud-scams

Remember: The IRS NEVER initiates initial email contact with tax professionals about returns, refunds, or requests for sensitive financial or password information.

Install Anti-Virus/Malware Software

Avoid FREE Anti-Virus. Get a PAID Subscription. FREE Software introduces unwanted Software and Ads.



Ensure it incorporates multi-protection layers to include firewall, Real-Time Scanning, Automatic Updates, Scheduled Scans, Anti-Spam, and Parental Controls.

Ensure it offers all inclusive protection mechanisms to address Viruses, Trojans, Worms, Spyware, Rootkits, Ransomware, Adware, Network attacks, and Web threats.

Ensure it is reliable by reviewing consumer reviews to ensure it protects without causing conflicts, safeguards its processes from unwanted termination, incorporates up-to-date protection, and integrates automated security scans.

Ensure it is easy to use and understand and it incorporates easy to find instructional documentation.

Use Strong & Unique Passwords

Eight (8) Characters or Longer.

Don't use personal data.
Don't use pet names.
Don't use dictionary words.

Mix of Lower and Upper Letters
Mix of Number (1,7,5)
Mix of Special Characters (#%*>)

Never share the password, not even with Help Desk.

Use Long Phrase
Mix Languages [dictionary vs. pronunciation limits cracking]

Set-up Two-Factor Authentication (2FA)

WEAK Password	STRONG Password
John123	SoMe^WheRe>OUt#TheRe*
P@$$word	HaV!T1EROMA-WeN
JosuaStreet345	GuT6nBu3no$G!orn>

NOTE: Password Generators are a great option; however, never use a password generator that's attached to a website. Also, never try to validate the strength of your password on a website claiming to validate it. It's a phishing mechanism to generate a list of passwords for hacking purposes.

Encrypt All Sensitive Files & Emails

When encrypting a file, keep in mind the following:

- ❑ Use of AES256+ algorithm or higher
- ❑ Use of Strong Password [See Password Requirements]
- ❑ Avoid using Online Encryption websites. Use encryption software that can be downloaded to your desktop and that is deemed trustworthy. Review consumer input.

Encrypt your text online — **CLEAR TEXT**

Hello,

This message has been encrypted using an online website; however, this action is not advisable. Is best to use a software that can be downloaded and executed offline on your desktop at all times, because the message encryption performed online via an untrusted site cannot be guaranteed and will hinder the encryption's file integrity.

Sincerely,

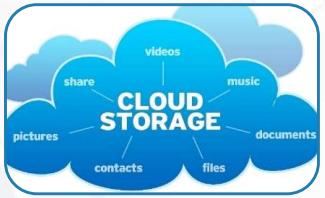
Karen Baez
CyberAdeptness LLC

Encrypt your text online — **ENCRYPTED**

EnCt21ca2ecab58f371519dddf7b4fc127c16f6182bb11ca2ecab58f371519dddf7b4s8LLvrP=TgO
M7t6Q3Fu5hefSMTagX3m3glro5lfEb1D0SHLIC3ARqt2+PScKHsyddJkQhKNSFLD52bcZwM00SnoVq1h
pl3j87OGBZbEsZKMD8HWyX8bBqMjlpPghZy43ebEe6xVce4/9SxHkff4eV2XRA7wd8bxVENdFOc8+/GJ
Lep0t1iFeFOCiUame+/A9s4t4swPL5LiT77CvHrOsMQu1w6TELbqm0Ol7WY3pN5U0RDEZ2fNUx4aQnM3
V2YXBIxiMETkyuxv3y6UUtrSD20kvlBjtkDYernsZb33L4Y4y46xY1XihgBVAir+6iYDA8smLsm4o5Dx
MArrzMxVZfzTsIYKoF81/3uDfsOx3qazO76MEUfR3Ir3/MxyMAdXGApsDpZzU+DMggGZqQM19AhwhZlh
WuFdEF3pTeNJ8Ypw/wXbsHr/sWvsQEuWc5a3zudpjP7wePH7BSPzO8ZBuYIniWcQcRFbIteWE3DoTbFe
aXYylEdRYv/u/O9hjUPMU7BR6ShA7ITBYMvNppOxpfV/flwEmS

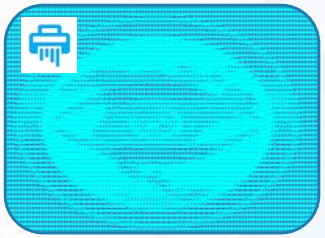
Decrypt file

Back-up Data



Universal Storage Bus	External Hard Drive	Cloud Storage
PROS: ▪ Small and Portable. ▪ Most offer full Encryption Protection. **CONS:** ▪ Can be lost easily. ▪ Must be connected to backup files. ▪ Cannot be left unattended, as it can be easily stolen. ▪ Must be carried along to access files.	**PROS:** ▪ Portable, but bulky. ▪ Perfect for Office. ▪ Most offer full Encryption Protection. ▪ Can be set-up for automatic backup in an office space, IF secured. **CONS:** ▪ Can be stolen. ▪ Must be carried along to access files.	**PROS:** ▪ Most are already Compliant with many Security Regulations impacting data security in the U.S. and Internationally. ▪ Accessible anywhere from the Web. **CONS:** ▪ There's a monthly cost for extra storage. ▪ Data must be extracted when the services are no longer paid for.

Wipe Or Destroy Old Equipment



Logical Data Sanitization	Physical Equipment Destruction
This includes data stored on: ▪ Portable Drives ▪ SD Cards ▪ Cloud Environment ▪ Desktop/Laptop Hard drives	This includes the following physical hardware: ▪ Portable Drives ▪ Hard Drives ▪ Memory (Printer and Devices) ▪ SD Cards ▪ CD's

NOTE: Before storing data in the cloud, determine the sanitization process employed by the provider. Encrypt all sensitive files if necessary prior to uploading.

Limit Equipment Access

Hardware Access	Logical Access
▪ Separate work computers from personal computers. ▪ Do not allow others to use the work computer. ▪ Store computers on a secured environment. Ideally locked down. ▪ Never allow someone to use your mobile devices IF they are used for work and contain sensitive data. ▪ Never leave unencrypted CDs, External Drives, or USBs out in the open. Make sure they are stored securely.	▪ Never give your access credentials to anyone, not even the help desk. ▪ Use Two Factor Authentication (2FA) whenever possible.

Wireless Network Security

Do not connect to a Public Network

Secure your home and office wireless network

Set-up Secured Tethering on Your Mobile Phone

Separate the wireless environments (if supported)

Data Theft

How to know if it happened.

Data Theft Clues

Data Theft can happen to anyone and is not always obvious. To determine if the data has been compromised, look for the following clues:

Return Rejected.
Social Security Already Filed.

No Tax Return Filed.
Authentication Letters (5071C, 4883c, 5747c) received from IRS.

No Tax Return Filed.
Tax Refund Received.

Tax Transcripts not requested received

IRS Account Accessed/Created
Notice from IRS or email denoting account is disabled received.

Number of clients for EFIN number exceeds those filed.

Unsolicited Emails Not Sent by Practitioner answered by client or tax professional.

Computer is Slower than Normal.
Cursor moving by itself.
Practitioner account locked down.

Stay Vigilant

Track daily e-file acknowledgements.
Track weekly EFIN usage.

Check Preparer Tax Identification Number (PTIN) Account for weekly report of returns filed under it.

Make sure the Centralized Authorization File (CAF) Number authorization is up-to-date.

Active two-factor authentication on all IRS Online Accounts, to prevent account takeover.

Reporting Data Breaches

Step by Step

Report Suspected or Actual Data Theft

- **Internal Revenue Service (IRS)**
- **State Tax Agencies**
  Email: StateAlert@taxadmin.org
- **Federal Bureau of Investigation (FBI)**
- **Cybersecurity Expert**
- **U.S. Secret Service**
- **Insurance Policy**
- **Local Police**
- **Credit Bureaus (Experian, Equifax, Transunion)**
- **Federal Trade Commission**
  Email: idt-brt@ftc.gov
- **Clients**

Go to https://www.irs.gov/individuals/data-theft-information-for-tax-professionals for a complete list.

Stay Connected with IRS

E-news For Tax PROS

Get the latest national and local IRS news.
Subscribe at
https://www.irs.gov/e-file-providers/join-e-news-for-tax-professionals

Quick Alerts

Stay up to date on the events that affect Authorized IRS *e-file* Providers and Issuers/Payers, Transmitters and Software Developers that will electronically file Affordable Care Act Information Returns.

Subscribe at
https://www.irs.gov/e-file-providers/subscribe-to-quick-alerts

Social Media

Twitter.com/IRStaxpros
Twitter.com/IRSnews

Facebook.com/IRStaxpros

How can CyberAdeptness Help?

Develop Security Documentation

Secure the environment

Validate Compliance

Sanitize or Destroy Equipment

Maintain the Systems and Documentation up-to-date.

Where can I find more information?

You may acquire additional information and stay up to date by…

- ***Visiting IRS Safeguard Website regularly*** [https://www.irs.gov/privacy-disclosure/safeguards-program]. This website maintains many resources to assist agencies with meeting Publication 1075 requirements. Examples of the website's features include:
  - Safeguard alerts and technical assistance documents
  - Recommendations on how to comply with Publication 1075 requirements
  - Reporting requirement templates (e.g., SSR) and guidance
  - Instructions for reporting unauthorized accesses, disclosures, or data breaches
  - Internal inspections report templates and instructions 24
  - IRS disclosure awareness videos and resources
  - Review Preparation Questionnaire (RPQ)
  - Cybersecurity requirements documented in Safeguard Computer Security Evaluation Matrix (SCSEM) templates organized by technology or topic
  - Nessus audit files
- ***Emailing IRS Safeguard's mailbox*** to attain additional information and/or submit reports at SafeguardReports@irs.gov . **Please note that this mailbox should be use for the following purposes only:**
  - Safeguards Reports and Extension Requests
  - 45-Day Notifications
  - Publication 1075 Technical Inquiries
  - Re-Disclosure Agreements
  - Data Incident Reporting
  - Ad hoc Points of Contact changes

Send them to
info@cyberadeptness.com

Need Help?

We have over 20+ years of combined experience in the field and a unique process to streamline the requirements.

Contact us today to schedule a meeting and determine how we may be of help to your organization. Our processes are flexible to accommodate compliance needs, regardless of sector (i.e., Healthcare, Finance, Law, Education, etc.).

References

- **IRS Publication 5293- Safeguarding Taxpayer Data: A Guide for your Business**- https://www.irs.gov/pub/irs-pdf/p5293.pdf
- **IRS Publication 4557- Safeguarding Taxpayer Data: A Guide for your Business-** https://www.irs.gov/pub/irs-pdf/p4557.pdf
- **IRS Publication 1345- Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns**- https://www.irs.gov/pub/irs-pdf/p1345.pdf
- **DHS Creating a Password Tip Card** - https://www.dhs.gov/sites/default/files/publications/Best%20Practices%20for%20Creating%20a%20Password.pdf

NOTE: Some items from the documents summarized have additional references. For detail information, review the documents above.