



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

11.3.36

FEBRUARY 24, 2025

EFFECTIVE DATE

(02-24-2025)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 11.3.36, Disclosure of Official Information, Safeguard Review Program.

MATERIAL CHANGES

- (1) Added internal controls subsections numbered IRM 11.3.36.1 through 11.3.36.1.5 and renumbered subsequent subsections accordingly. Titled IRM 11.3.36.1 Program Scope and Objectives, to properly reflect the information communicated in this subsection. Information from prior subsections 11.3.36.3, Legal Requirements, and 11.3.36.6, Responsibilities, were incorporated into the revised subsections. Also included important information to conform to the new internal and management control standards under the following titles:
 - a. IRM 11.3.36.1.1 - Background
 - b. IRM 11.3.36.1.2 - Authority
 - c. IRM 11.3.36.1.3 - Roles and Responsibilities
 - d. IRM 11.3.36.1.4 - Terms/Definitions/Acronyms
 - e. IRM 11.3.36.1.5 - Related Resources
- (2) Added use of Safeguards SharePoint Online to IRM 11.3.36.1.5, Related Resources.
- (3) Added communications to IRM 11.3.36.1.5, Related Resources.
- (4) Added documentation requirements on workstreams for Safeguards' electronic case management system to IRM 11.3.36.4, Documentation.
- (5) Added time tracking requirements for the electronic case management system to IRM 11.3.36.4, Documentation.
- (6) Added the requirement to use naming conventions to IRM 11.3.36.4, Documentation.
- (7) Combined IRM 11.3.36.6, SSR Analysis into IRM 11.3.36.5, Initial and Annual Safeguard Security Report (SSR) and renumbered subsequent subsections accordingly.
- (8) Updated the format of instructions for the following workstreams to include assignment, analysis, and processing:
 - a. IRM 11.3.36.8 – Corrective Action Plans
 - b. IRM 11.3.36.9 – Technical Inquiries
 - c. IRM 11.3.36.10 – 45 Day Notifications
- (9) Combined IRM 11.3.36.13, State and Local Agency Review and IRM 11.3.36.14, Federal Agency Reviews into IRM 11.3.36.12, Safeguard Reviews and renumbered subsequent subsections accordingly.
- (10) Removed IRM 11.3.36.16, Safeguards Mailbox and Secure Data Transfer subsection used as a placeholder.
- (11) Updated various subsections of IRM 11.3.36 to correct inconsistencies in terms and acronyms associated with core workstreams.

- (12) Updated various subsections of IRM 11.3.36 to remove the specific names expressed associated with the electronic inventory management application utilized and the contractor computer security support provider.
- (13) Updated various subsections of IRM 11.3.36 with accurate and consistent expressions of statutes, procedures, and regulations.
- (14) Removed the following IRM Exhibits:
 - a. IRM Exhibit 11.3.36-1, Safeguard Evaluation Guide
 - b. IRM Exhibit 11.3.36-2, Safeguard Review Report Format - Findings and Recommendations
 - c. IRM Exhibit 11.3.36-3, QR SRR Preparation Check Sheet
 - d. IRM Exhibit 11.3.36-4, QR of TI Preparation Check Sheet
 - e. IRM Exhibit 11.3.36-5, QR SSR Preparation Check Sheet
 - f. IRM Exhibit 11.3.36-6, QR CAP Preparation Check Sheet
 - g. IRM Exhibit 11.3.36-7 Artifacts for Review
- (15) Removed IRM Exhibit 11.3.36-8 and incorporated information requirements into IRM 11.3.36.16.4, Associate Directors Actions.

EFFECT ON OTHER DOCUMENTS

This material supersedes IRM 11.3.36, Safeguard Review Program, dated July 21, 2015.

AUDIENCE

Office of Safeguards employees.

Celia Y. Doggette
Director, Governmental Liaison, Disclosure and Safeguards
(GLDS)

11.3.36

Safeguard Review Program

Table of Contents

11.3.36.1 Program Scope and Objectives

11.3.36.1.1 Background

11.3.36.1.2 Authority

11.3.36.1.3 Roles and Responsibilities

11.3.36.1.4 Program Management

11.3.36.1.5 Program Controls

11.3.36.1.6 Terms/Definitions/Acronyms

11.3.36.1.7 Related Resources

11.3.36.2 Awareness

11.3.36.3 Implementing Requirements

11.3.36.4 Documentation

11.3.36.5 Initial and Annual Safeguard Security Report (SSR)

11.3.36.5.1 Initial SSR

11.3.36.5.2 Content of Initial SSR

11.3.36.5.3 Annual SSR Preparation Guidelines

11.3.36.5.4 Annual SSR Content

11.3.36.5.5 SSR Assignment

11.3.36.5.6 SSR Analysis

11.3.36.5.7 SSR Processing

11.3.36.5.8 Delinquent or Incomplete Annual SSRs

11.3.36.6 Safeguard Review Preliminary Findings Report (PFR)

11.3.36.7 Safeguard Review Reports (SRR)

11.3.36.7.1 SRR Content

11.3.36.7.2 SRR Processing Procedures

11.3.36.8 Corrective Action Plan (CAP)

11.3.36.8.1 CAP Assignment

11.3.36.8.2 CAP Analysis

11.3.36.8.3 CAP Processing

11.3.36.9 Technical Inquires (TI)

11.3.36.9.1 TI Assignment

11.3.36.9.2 TI Analysis

11.3.36.9.3 TI Processing Procedures

11.3.36.10 45 Day Notifications

11.3.36.10.1 Agency Submission of 45 Day Notification and Correspondence

11.3.36.10.2 Notification Assignments

-
- 11.3.36.10.3 45 Day Notification Analysis
 - 11.3.36.10.4 45 Day Notification Processing
 - 11.3.36.11 Quality Review
 - 11.3.36.11.1 Quality Review of Safeguard Security Reports
 - 11.3.36.11.2 Quality Review of Safeguard Review Reports
 - 11.3.36.11.3 Quality Review of Technical Inquires
 - 11.3.36.11.4 Quality Review of 45 Day Notifications
 - 11.3.36.12 Safeguard Reviews
 - 11.3.36.12.1 Safeguard Review Preparation
 - 11.3.36.12.2 Conducting the Safeguard Review
 - 11.3.36.12.3 Review Techniques
 - 11.3.36.12.4 Team Coordination
 - 11.3.36.12.5 Need and Use Reviews
 - 11.3.36.12.6 Preliminary Findings Report Preparation
 - 11.3.36.12.7 Closing Conference
 - 11.3.36.12.8 Work Papers
 - 11.3.36.13 Inventory and Management Reports
 - 11.3.36.13.1 Technical Inquires and Notifications
 - 11.3.36.13.2 Safeguards Review Report
 - 11.3.36.13.3 Safeguards Security Report
 - 11.3.36.13.4 Corrective Action Plan
 - 11.3.36.14 Management Information Reports
 - 11.3.36.15 Report to Congress
 - 11.3.36.16 Enforcement
 - 11.3.36.16.1 Guidelines for Safeguards Task Alliance Team (STAT) Enforcement of Safeguard Reporting Requirements
 - 11.3.36.16.2 Guidelines for Safeguard Review Team (SRT) Enforcement of Safeguard Requirements Other Than Reporting
 - 11.3.36.16.3 Enforcement Actions of Safeguard Requirements Other Than Reporting
 - 11.3.36.16.4 Associate Director's Actions
 - 11.3.36.16.5 Alternative Actions

11.3.36.1
(02-24-2025)
Program Scope and Objectives

- (1) **Purpose:** This IRM provides instructions to Office of Safeguard personnel when performing casework, safeguard evaluations, and reviews.
- (2) **Audience:** Office of Safeguard employees. Agencies with which IRS shares Federal tax return and return information follow Publication 1075, Tax Information Security Guidance for Federal, State, and Local Agencies.
- (3) **Policy Owner:** The Government Liaison, Disclosure and Safeguards (GLDS) office, under Privacy, Government Liaison and Disclosure (PGLD), is the program office responsible for oversight of Office of Safeguard policy.
- (4) **Program Owner:** Office of Safeguards, under GLDS, is responsible for oversight of external agencies compliance with the safeguarding requirements that protect the confidentiality of Federal Tax Information (FTI) when IRS shares tax information as authorized by law.
- (5) **Primary Stakeholders:** Office of Safeguards in collaboration with federal agencies, bodies, commissions, or state agencies receiving FTI subject to IRS oversight under IRC 6103(p)(4).

11.3.36.1.1
(02-24-2025)
Background

- (1) The Office of Safeguards is responsible for ensuring agency and contractor personnel authorized to access Federal tax return information - collectively termed FTI – maintain adequate safeguards for the protection of such information. Written procedures and instructional guidelines are included to help the reviewer determine whether the agency and contractor personnel provide adequate protection for FTI consistent with the Department of Treasury and IRS guidelines, manuals and regulations.
- (2) The program is a cooperative effort with the recipient agencies and contractors to ensure the confidentiality of FTI. Outreach and communication are key elements in promoting protection of FTI. In order to fulfill legal requirements and IRS responsibilities, the program must also maintain viable enforceable standards and full time enforcement.

Note: The term agency includes Federal, state and local agencies, entities, and agency contractors. The term contractor will generally reference agency contractor, while IRS contractors will specifically be referred to as IRS contractors.

11.3.36.1.2
(02-24-2025)
Authority

- (1) IRC 6103 and IRC 6104(c) permit IRS to enter into agreements to disclose FTI to various Federal, state, and local agencies.
- (2) IRC 6103(p)(4) requires the agencies receiving tax returns and return information under specific disclosure provisions provide adequate safeguards to protect the confidentiality of the tax returns and return information to the satisfaction of the Secretary (of Treasury) as a condition of receiving FTI.
- (3) IRC 6103(p)(4)(E) requires that any federal agency, body, commission, or state agency receiving FTI subject to IRS oversight under IRC 6103(p)(4) submit reports to the Office of Safeguards that describe the procedures established for ensuring the confidentiality of FTI. For monitoring and reporting purposes, the agencies are categorized by the authority to receive FTI as one of the following:
 - Federal Agencies

- State Attorney General (AG)
- State Departments of Revenue (DOR)
- State and Local Child Support (CS) Enforcement Agencies
- State Human Services (HS) Agencies
- State Departments of Transportation (DOT)
- State Workforce Agencies (SWA)
- State Affordable Care Act (ACA)

Note: This also pertains to any agency, lender, and institution disclosing mailing addresses received pursuant to IRC 6103(l)(6)(A), IRC 6103(l)(12)(B), IRC 6103(m)(2), IRC 6103(m)(4), IRC 6103(m)(6), or IRC 6103(m)(7) to its agent(s) and contractor(s).

- (4) IRC 6103(p)(5) requires the Commissioner to furnish annual reports to the House Committee on Ways and Means, the Senate Committee on Finance and the Joint Committee on Taxation. The reports describe procedures and safeguards established by the various agencies and their respective contractors who receive FTI, as well as indicating deficiencies on the part of the agencies and their contractors.
- (5) IRC 6103(p)(7) establishes a process for the suspension or termination of FTI and an administrative review if an authorized recipient has failed to safeguard returns or return information.
- (6) IRC 6103(p)(8) contains confidentiality protections for copies of Federal tax returns, or portions thereof, attached to State tax returns, or the Federal return information reflected on a State tax return supplied by a taxpayer pursuant to a state requirement.

Note: See IRM 11.3.36.12, Safeguard Reviews for additional information.

- (7) IRC 6103(p)(9) requires that agencies disclosing tax returns and return information under specific disclosure provisions to contractors provide adequate safeguards to protect the confidentiality of the tax returns and return information to the satisfaction of the Secretary (of Treasury). For monitoring and reporting purposes, the agency must ensure the following:

- Conduct on-site reviews of the contractor to determine compliance.
- Submit findings from the most recent on-site review to Safeguards annually.
- Certify contractors are following Safeguards requirements annually.

Note: See also IRM 11.3.36.5, Initial and Annual Safeguard Security Report (SSR).

- (8) IRC 7213 provides criminal penalties for unauthorized disclosures of FTI.
- (9) IRC 7213A provides criminal penalties for unauthorized inspections of FTI.
- (10) IRC 7431 provides civil remedies for unauthorized disclosures and inspections of FTI.
- (11) Title 26 Code of Federal Regulations (CFR) 301.6103(n)-1(e) authorize the IRS to determine the safeguards compliance of agency contractors.
- (12) Title 26 CFR 301.6103(p)(4)-1 refers to IRS published guidance regarding security guidelines and other safeguards for protecting FTI.

- (13) Title 26 CFR 301.6103(p)(7)-1 addresses procedures for administrative review of a determination that an authorized recipient has failed to safeguard FTI.
- (14) See also IRM Exhibit 10.8.1-2, Information Technology (IT) Security Policy and Guidance for applicable security laws and regulations, and other guidance.

11.3.36.1.3
(02-24-2025)
**Roles and
Responsibilities**

- (1) The Office of Safeguards is responsible for ensuring that external agencies authorized to receive FTI maintain proper safeguards to adequately protect the data. Agencies receiving return information and the authorized contractors must protect the confidentiality of return information and are periodically reviewed by Office of Safeguards personnel to ensure they meet the safeguarding requirements of IRC 6103(p)(4). These requirements include:
 - Record Keeping
 - Secure Storage
 - Restricting Access
 - Other Safeguard Measures
 - Reporting
 - Disposal
 - Information Technology Security and Privacy
- (2) The Associate Director (AD), Office of Safeguards, reports to the Director, GLDS, and oversees the Safeguard program. The following Office of Safeguards managers and staff report directly to the AD:
 - Review Team Area Manager (AM)
 - Technical Advisors (TA)
 - Supervisory Management & Program Analyst, Safeguards Policy Team (SPT)
 - Supervisory Management & Program Analyst, Strategy and Risk Team (S&RT)
- (3) The following Office of Safeguards managers and staff report to the AM:
 - Supervisory Disclosure Enforcement Specialist (DES), Safeguards Review Teams (SRT) 1 and 2
 - Supervisory DES, Federal Review Team (FRT)
 - Information Technology Specialist (ITS) TA
 - Management and Program Analyst (MPA) TA
- (4) The following Office of Safeguards staff report to the Supervisory DES, SRT/ FRT:
 - DES
 - ITS
 - Management Assistant (MA)
- (5) The following Office of Safeguards staff report to the Supervisory Management & Program Analyst, SPT:
 - ITS
 - MPA
 - MA
 - Policy Analyst (PA)
 - Program Evaluation and Risk Analyst (PERA)

- (6) The following Office of Safeguards staff report to the Supervisory Management & Program Analyst, S&RT:
 - Computer Engineer (CE)
 - ITS
 - MPA
 - PA
 - PERA
- (7) IRS IT contractors are used for case work involving computer security requirements. IRS IT contract responsibilities are listed in the IT Security Support Services Contract.
- (8) Agencies receiving FTI are responsible for following the safeguarding requirements in Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies.

11.3.36.1.4
(02-24-2025)

Program Management

- (1) Implementation of the Safeguards Program relies on a coordinated effort between SPT, S&RT, and the SRT/FRT.
- (2) Safeguards Policy Team: Ensures compliance with laws and regulations, gives guidance for decision-making, and streamlines internal processes.
- (3) Strategy & Risk Team: Identifies risks associated with non-compliance, assesses risk, mitigates risk, and finds risk mitigation solutions.
- (4) Safeguard Review Teams: Review Teams 1 and 2 ensure compliance with safeguarding requirements of state and local agencies receiving FTI by conducting safeguard reviews and preparing safeguard review reports.
- (5) Federal Review Team: Ensure compliance with safeguarding requirements of federal agencies receiving FTI by conducting safeguard reviews and preparing safeguard review reports.

11.3.36.1.5
(02-24-2025)

Program Controls

- (1) The Office of Safeguards reports program updates in regular Operational Reviews with the Director of PGLD.
- (2) The Office of Safeguards operates and controls access to its eCase, *Safeguards SharePoint Online*, and OneDrive for use in storing, developing and sharing documents within the function and with IRS reviewers on an as needed basis.

11.3.36.1.6
(02-24-2025)

**Terms/Definitions/
Acronyms**

- (1) The tables below list commonly used terms, definitions and acronyms used throughout this IRM section:

Term	Definition
Access	<ol style="list-style-type: none"> 1. The act of entering a restricted or locked area, room, container, or system containing FTI, or 2. The act of obtaining, acquiring, receiving, examining, using or gaining knowledge of FTI, by physical, electronic, or any other methods. <p>Example: Users (e.g., system administrators, database administrators) have access to FTI if they have the ability to modify or bypass security controls protecting FTI (to include decryption keys).</p>
Breach	The loss of control, disclosure, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where individuals other than authorized users and for other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.
Chief	Functional title for the Supervisory DES to reduce confusion and provide clarity to Safeguards' Review Teams.
Cyber Security Reviewer (CSR)	Functional title for ITS or IRS IT contractors which perform IT/ cyber analysis on casework and conducts the cyber portion of a Safeguards review. The functional title is used to reduce confusion and provide clarity to Safeguards' operations and documentation.

Term	Definition
Disclosure	The making known to any person in any manner whatever a return or return information. For example, confirming whether a tax return is on file or not (i.e. fact of filing) is a disclosure.
eCase	An electronic inventory management application containing records profiles of agency partners subject to IRC 6103(p)(4) oversight and the reporting submissions utilized to monitor their compliance meeting safeguard requirements.
Federal tax information (FTI)	Any return or return information protected by IRC 6103 confidentiality whether received from the IRS, or secondary source such as the Social Security Administration, etc. FTI includes any information created by a recipient agency that is derived from return or return information.
Loss	Any event where an item is misplaced and/or neither the official owner nor the intended recipient has possession of the item in the expected time frame.
Return	Any tax or information return, estimated tax declaration, or refund claim - including amendments, supplements, supporting schedules, attachments, or lists - required by or permitted under the IRC and filed with the IRS by, on behalf of, or with respect to any person or entity.
Return information	Generally any information collected or generated by the IRS with regard to any person's liability or possible liability under the IRC. IRC 6103(b)(2)(A) defines return information very broadly.

Acronym	Definition
ACA	Affordable Care Act

Acronym	Definition
ACI	Agency Contact Information
AD	Associate Director
AG	Attorney General
AM	Area Manager
AUSA	Assistant U.S. Attorney
BEER	Beneficiary Earning Exchange Record
CAP	Corrective Action Plan
CBO	Congressional Budget Office
CE	Computer Engineer
CFR	Code of Federal Regulations
CMA	Computer Matching Agreement
CS	Child Support
CSR	Cyber Security Reviewer
DES	Disclosure Enforcement Specialist
DI	Data Incident
DOR	Department of Revenue
DOT	Department of Transportation
FRS	Federal Review Scope
FRT	Federal Review Team
FTI	Federal tax information
GAO	Government Accountability Office
GL	Government Liaison
GLDEP	Government Liaison Data Exchange Program
GLDS	Government Liaison, Disclosure, Safeguards
HOA	Head of Agency
HS	Human Services
IEVS	Income and Eligibility Verification Systems
IRC	Internal Revenue Code
IT	Information Technology
ITS	Information Technology Specialist

Acronym	Definition
IVR	Interactive Voice Response
MA	Management Assistant
MOU	Memo of Understanding
MPA	Management Program Analyst
NIST	National Institute of Standards & Technology
OCSS	Office of Child Support Services
PA	Policy Analyst
PERA	Program Evaluation Risk Analyst
PFR	Preliminary Findings Report
PGLD	Privacy, Governmental Liaison and Disclosure
POA&M	Plan of Actions and Milestones
POC	Point of Contact
PSE	Preliminary Security Evaluation
QR	Quality Review
RPQ	Review Prep Questionnaire
S&RT	Strategy and Risk Team
SAR	Security Assessment Report
SCSEM	Safeguards Computer Security Evaluation Matrix
SDSEM	Safeguards Disclosure Security Evaluation Matrix
SDT	Secure Data Transfer
SLA	Service Level Agreement
SOI	Statistics of Income
SOP	Standard Operating Procedure
SPT	Safeguards Policy Team
SRT	Safeguards Review Team
SRR	Safeguard Review Report
SSA	Social Security Administration
SSR	Safeguard Security Report
STAT	Safeguards Task Alliance Team
SWA	State Workforce Agency

Acronym	Definition
TA	Technical Advisor
TDS	Transcript Delivery System
TFA	Taxpayer First Act
TI	Technical Inquiry
TIGTA	Treasury Inspector General for Tax Administration
TOC	Table of Contents
VoIP	Voice Over Internet Protocol

11.3.36.1.7
(02-24-2025)

Related Resources

- (1) Additional sources of guidance can also be found at the related resources:
 - IRM 11.3 series, Disclosure of Official Information
 - IRM 11.3.32, Disclosure to States for Tax Administration Purposes
 - IRM 11.3.29, Disclosure to Government Agencies for Administration of Non Tax Laws
 - National Institute of Standards & Technology (NIST) Special Publication (SP) 800- 53, Security and Privacy Controls for Information Systems and Organizations
- (2) *Safeguards SharePoint Online* Component:
 - A centralized repository maintained by SPT for standard operating procedures (SOP), instructions, templates and other necessary reference information for Safeguards staff when conducting work on workstreams.
 - Contains a variety of useful information and resources.
 - There is a "Search" box at the top of every SPO for searching files by keyword of the file name.
- (3) Safeguards effectively communicates with internal and external stakeholders, by:
 - Informing Safeguards external partners of updates and changes to the Safeguards program through Security & Privacy Alerts.
 - Conducting quarterly Office Hour Calls with external partners to discuss updates and changes to the Safeguards program.
 - Conducting Technical Calls with Safeguards staff to discuss updates and changes to the Safeguards Program.

11.3.36.2
(02-24-2025)
Awareness

- (1) When an agency receives, or expresses an interest in receiving, FTI ensure that the agency obtains a copy of IRS Publication 1075, **Tax Information Security Guidelines for Federal, State, and Local Agencies**. Copies of Publication 1075 can be obtain from <http://www.irs.gov/uac/Safeguards-Program>.

11.3.36.3
(02-24-2025)
**Implementing
Requirements**

- (1) Federal, State and local agencies must submit the following to the office of Safeguards:
 - a. Initial SSR and
 - b. Annual SSR
- (2) These reports are described in detail in IRM 11.3.36.5, Initial and Annual SSR.
- (3) The IRS reviews reports received from agencies to determine the adequacy of agency safeguards.
- (4) If an agency fails to submit the required report or to provide sufficient information to allow the IRS to determine the adequacy of its safeguards, the IRS can recommend withholding FTI from that agency. See also IRM 11.3.36.16, Enforcement for additional guidance.
- (5) Onsite Safeguard Reviews of agencies and contractors they authorize are outlined in IRM 11.3.36.12, Safeguard Reviews.

11.3.36.4
(02-24-2025)
Documentation

- (1) All steps taken in the review and report process must be documented within three business days of occurrence unless extenuating circumstances require additional time to complete documentation. All notes, worksheets, communication contacts, memoranda, and other correspondence supporting actions taken and determinations made must be retained in the case.
- (2) Safeguards use of an electronic case management system, also known as eCase, is used to document case work on all workstreams.
 - The electronic case management system must be used to document actions taken when working SSRs, Safeguard Review Reports (SRRs), Corrective Action Plans (CAPs), Technical Inquiries (TIs), 45 Day Notifications, and Data Incidents (DIs).
 - Case documents such as correspondence, reports, and work products must be uploaded as attachments in the electronic case management system when working SSRs, SRRs, CAPs, TIs, 45 Day Notifications, and DIs.
 - Case notes documenting actions must be input within three business days of occurrence unless extenuating circumstances required additional time to complete documentation.
 - Case notes must provide detailed information, which includes information on the following: facts, occurrence, plans, and actions taken.

Note: If an email is referenced in the case notes, then it must be attached to the applicable case.
 - Safeguards Staff must reference the Electronic Case Management System User Guides for information on creating cases, updating notes, uploading attachments, and importing data.
- (3) Case notes in the inventory management system must clearly define actions taken including: initial analysis steps, identification of records requested, and research completed. A case note must be made to refer to an action even though a form or document relative to the action is in the case file. Case note documentation must be:
 - Complete - Include all significant actions. Managerial and OJI involvement as well as other external/internal stakeholder communication must

- be documented using full names, explanation of who the person is, and phone numbers, emails, or other contact information used for external contacts.
- Coherent - Use plain language and proper grammar. Do not use acronyms or abbreviations that are not commonly understood.
 - Timely - Document all case actions as they take place to ensure case notes are accurately updated in a timely manner. Contemporaneous case note documentation is part of workload management and if done timely and correctly will save time on cases. Taking timely substantive action on casework and documenting those actions, including reason(s) for delays, help mitigate risks. Periods of inactivity must be explained. Entries must be made in chronological order and recorded the day the action occurs or as soon as practicable thereafter.
 - Relevant - Stick to the facts. Do not document personal observations, speculation or opinions.
- (4) Safeguards uses the following naming convention to assist in correctly naming documents uploaded to the electronic case management system such as SSRs, SRRs, CAPs, TIs, 45 Day Notifications, and DIs.
1. Agency Code
 2. Agency Type
 3. Type of Document
 4. Secondary Document Type
 5. Date

Example: MAXXX-DOR-SRR-062923

11.3.36.5
(02-24-2025)
**Initial and Annual
Safeguard Security
Report (SSR)**

- (1) IRC 6103(p)(4)(E) requires agencies receiving FTI to file an SSR that describes the procedures established and used by the agency for ensuring the confidentiality of the information received from the IRS or obtained through an authorized secondary source such as Social Security Administration (SSA), Federal Office of Child Support Services (OCSS), Bureau of the Fiscal Services (BFS) or Centers for Medicare and Medicaid Services (CMS). The SSR records how the agency utilizes FTI and the security controls in place to protect FTI from unauthorized access and disclosure. The agency shall file a SSR in accordance with Publication 1075, Section 2.E.4.4, SSR Submission Dates.
- (2) The SSR must include:
- Certification that the agency is protecting FTI pursuant to IRC 6103(p)(4) and the agency's own security requirements.
 - Summary of the agency's current efforts to ensure the confidentiality of FTI.
 - Modifications/changes to the procedures or safeguards described in a previous SSR.
 - Future actions that will affect the agency's safeguard procedures.
 - Taxpayer First Act (TFA) 2004 Legislation Required Documentation.

Note: SSRs must be approved prior to initial release of FTI to agencies.

- (3) **Disclosures Under Multiple Code Sections (Federal Agencies)** – Some Federal agencies receive FTI from the IRS under the authority of more than one section of the IRC. In these cases, the agency must distinguish between

the IRC sections, and provide safeguard procedures for each program or use. The agency must file a consolidated SSR for the various programs or uses.

- (4) Federal, state, and local agencies using Form 8300, Report of Cash Payments Over \$10,000 Received in a Trade or Business, available information pursuant to IRC 6103(l)(15) must file a separate SSR for this program. All agencies requesting data under IRC 6103(l)(15) are referred to the Office of Safeguards.

Note: Where IRS/CI and the U.S. Attorney's Office are among the participants of a multi-agency task force, and there is an investigative need to obtain Form 8300 information, the Assistant U.S. Attorney (AUSA) assigned to the task force is the requestor of information. Safeguards for FTI safeguarding will therefore be centralized with the AUSA's office

- (5) Safeguards staff must reference IRM 11.3.36.4, Documentation and IRM 11.3.36.1.7, Related Resources for additional information on working SSRs.

11.3.36.5.1 (02-24-2025) Initial SSR

- (1) Agencies executing data exchange agreements involving access to FTI will be subject to safeguarding requirements and must provide evidence that adequate safeguard protections and controls are in place before the IRS will authorize the release of FTI. The agency must submit an initial SSR for approval at least 90 days prior to the agency's planned FTI receipt date.
- (2) In order to obtain initial IRS approval to receive FTI, an agency must have an approved SSR. To facilitate IRS approval, the agency is expected to:
 - Designate an agency Safeguards Point of Contact (POC)
 - Make program officials, contractors, and/or subcontractors available to discuss access and use of FTI, as needed.
- (3) The agency is required to submit evidentiary documentation for the controls identified in Publication 1075, Section 2.E.4.1, Table 3 in conjunction with the first submission of the agency's SSR.
- (4) If the agency does not submit all required evidentiary documentation as described above, the IRS reserves the right to conduct a safeguard review to assess the effectiveness of the controls established in order to approve the SSR prior to initial release of FTI. Subsequently, Safeguards will conduct a risk-based assessment to determine when to schedule an agency's first safeguard review after initial receipt of FTI.
- (5) The agency must address all elements in the SSR template, additionally the initial SSR must contain the evidence, Artifacts for Review, which focus on:
 - a. Controls that in their absence would potentially leave FTI exposed to a threat
 - b. IRS-specific controls that are critical for the protection of FTI.
 - c. Security Assessment Report (SAR) indicating the system is configured to minimize risk to FTI.
- (6) The Office of Safeguards will perform a comprehensive review of the agency's entire SSR and each control description for compliance with standards to understand the agency's overall security posture before approving the SSR and request additional artifacts as needed.

11.3.36.5.2
(02-24-2025)

Content of Initial SSR

(1) **General:**

- a. Responsible officers or employees.
- b. Functional organizations using the data.
- c. Computer facilities or equipment and system security.
- d. Physical security.
- e. Retention policy and disposal methods.

(2) **Safeguard activities** shall include, at a minimum, the following items:

- a. **Functional organizations using the data**
- b. **Computer Facilities or Equipment and System Security** – Changes or enhancements.
- c. **Physical Security**– Changes or enhancements.

(3) **Agency Disclosure Awareness Program** – The agency must describe the efforts to inform all employees having access to FTI of the confidentiality requirements of the IRC, the agency's security requirements, and the sanctions imposed for unauthorized inspection or disclosure of return information.

(4) **Reports of Internal Inspections** – The agency must provide copies of a representative sampling of the Inspection Reports and a narrative of the corrective actions taken (or planned) to correct any deficiencies must be included with the annual SSR.

(5) **Disposal of FTI** – The agency must report the disposal or return of FTI to the IRS or source. The information must be adequate to identify the material destroyed and the date and manner of destruction, including copies of destruction logs.

Note: Including taxpayer information in the disposal record is not necessary and must be avoided.

(6) **Other information** –The agency must provide other information to support the protection of FTI, in accordance with IRC 6103(p)(4) requirements.

(7) **Planned Actions Affecting Safeguard Procedures** – Any planned agency or contractor action which would create a major change to current agency procedures or safeguards must be reported. Such major changes would include, but are not limited to, new computer equipment, facilities or systems to perform programming, processing or administrative services requiring access to FTI.

(8) **Agency Use of Contractors** – Agencies must account for the use of all contractors, permitted by law or regulation, to do programming processing or administrative services requiring access to FTI. Agencies must identify all contractors requiring access to FTI on the TFA 2004 Contractor Worksheet attached with the SSR and must certify the identified contractors have safeguards in effect to ensure FTI is kept confidential.

(9) **On Boarding** – As part of the on boarding process, new agencies are required to have an approved SSR, Security Assessment Report (SAR) and Authority To Operate (ATO) before receiving FTI.

(10) **Safeguard Security Report Signed Certification Page**

- Submissions must include a signed certification letter from the Head of Agency or a designee. In the event the agency submits a report signed by a designee, there must be a delegation of authority signed by the Head of Agency (HOA).
- All correspondence requiring HOA signature must be in the form of a handwritten (aka. Wet) signature or a digital certificate signature. The HOA can delegate individuals to sign these documents on their behalf. To do so, the HOA must provide a delegation of authority for the individual they will assign as their designee. The delegation of authority must be kept current by the agency and retained for at least three years and will be reviewed by IRS personnel during Safeguard reviews.

11.3.36.5.3
(02-24-2025)
Annual SSR Preparation Guidelines

- (1) Preparation of an Annual SSR begins with a review of the previous SSR submission to:
 - Cover outstanding actions list;
 - Identify areas where there is no change;
 - Identify areas that are not applicable; and
 - Address content changes
- (2) When an agency requests an extension to file their annual SSR, refer them *Publication 1075 , Section 2.E.4.4, SSR Update Submission Dates*

11.3.36.5.4
(02-24-2025)
Annual SSR Content

- (1) Agencies are required to submit an annual SSR encompassing any changes that impact the protection of FTI:
 - New data exchange agreements.
 - New computer equipment, systems, or applications (hardware or software).
 - New facilities; and
 - Organization changes, such as moving IT operations to a consolidated data center from an embedded IT operation.
- (2) The SSR must reflect updates or changes in the agency or safeguarding procedures within the reporting period to include:
 - Changes to information or procedures previously reported;
 - Current annual period safeguard activities;
 - Planned actions impacting safeguard procedures; and
 - Agency use of contractors (non-agency employees).
- (3) The SSR must document IRC 6103(p)(9) requirements that contractors, sub-contractors, or other agents have requirements in effect to provide safeguards required under IRC 6103(p)(4) by including the following:
 - Certification for the most recent annual period that agency contractors (or other agents with access to FTI), which were reviewed during the reporting period, are minimizing risk to FTI as required by Publication 1075.
 - Identify all agency contractors (or other agents with access to FTI) on the TFA 2004 Contractor Worksheet.
 - Document the findings for each onsite review completed during the SSR reporting period on the TFA 2004 On-Site Review Template.
- (4) The following are criteria for SSR attachments:

- File attachments must clearly identify the filename and section contained within the attachment being referenced.
- Attachment filenames must follow a standardized naming convention by a logical order (e.g., SSRATT1, SSRATT2).
- Attachments must not be embedded into the SSR.

(5) Safeguard Security Report Signed Certification Page

- Submissions must include a signed certification letter from the HOA or a designee. In the event the agency submits a report signed by a designee, there must be a delegation of authority signed by the HOA.
- All correspondence requiring HOA signature must be in the form of a handwritten (aka. Wet) signature or a digital certificate signature. The HOA can delegate individuals to sign these documents on their behalf. To do so, the HOA must provide a delegation of authority for the individual they will assign as their designee. The delegation of authority must be kept current by the agency and retained for at least three years and will be reviewed by IRS personnel during Safeguard reviews.

(6) Location of the Data – Include an organization chart or narrative description of the receiving agency organization, which includes all functions where FTI is processed or maintained. If the FTI is used or processed by more than one function, then pertinent information about each function must be included.

(7) Flow of the Data – The report must contain a flow chart or narrative description of:

- a. The flow of the FTI data from receipt through its return to the IRS or its final destruction;
- b. How FTI is to be used or processed;
- c. How FTI is tracked and protected as it moves within and outside the agency;
- d. Describe how FTI is commingled with or separated from agency data;
- e. Describe the paper or electronic products created from FTI; and
- f. Where contractors are involved in the flow of FTI including when authorized by statute or regulation.

(8) System of Records – A description of the permanent record(s) used to document requests for, receipt of, dissemination of (if applicable), and final disposition (return to the IRS or destruction) of the FTI (including all electronic media). Agencies and their contractors are expected to be able to provide an “audit trail” for all FTI requested and received. Audit trails must account for copies made or distribution of the original document/media receipts.

(9) Secure Storage of the Data – A description of the security measures employed to provide secure storage for the FTI when it is not being used. Secure storage encompasses such diverse considerations as locked files or containers, secured facilities, key or combination control, off-site data storage facilities, and restricted areas.

(10) Restricting Access to the Data – A description of the procedures or safeguards to ensure access of FTI is limited to those individuals authorized access and have a need to know. Describe any physical barriers protecting FTI from unauthorized access when in use by the authorized individual including all security features where FTI is accessed, used or processed as well as any systemic and or procedural barriers.

- (11) Disposal – A description of disposal, including method of disposal for FTI provided by IRS and/or produced by the agency or contractor (e.g., print-outs, back-up tapes and the like). (See paragraph (8), System of Records above)
- (12) Information Technology Security – A description of all automated information systems and networks that receive, process, store, or transmit FTI. All systems are required to have safeguard measures in place which address all key components of IT security to restrict access to sensitive data, see Publication 1075, Sections 3.0 and 4.0. The description must include:
 - a. Systemic controls employed to ensure all FTI is safeguarded from unauthorized access or disclosure;
 - b. Procedures to be employed to ensure secure storage of the disks and the data, limit access to the disk(s) or computer screens, and the destruction of the data;
 - c. Additional comments regarding the safeguards employed to ensure the protection of computers;
 - d. Security precautions undertaken if the agency's computer systems are connected or planned to be connected to other systems; and
 - e. Procedures for ensuring that all data is safeguarded from unauthorized access or disclosure.
- (13) Disclosure Awareness Program – Description of the formal awareness program each agency and contractor who receives FTI has, where employees with access to FTI certify annually the training received and receipt of the confidentiality provisions of the IRC including the civil and criminal sanctions for unauthorized inspections or disclosures of FTI.

11.3.36.5.5
(02-24-2025)
SSR Assignment

- (1) Mailbox Staff must take the following actions when a SSR is received in the mailbox:
 - a. Retrieve the SSR and create a case in the electronic case management system within 3 business days from mailbox receipt.
 - b. Upload the agency SSR and attachments into the case.

Note: Attachments in the electronic case management system must not be password protected.

 - c. Review the SSR to make sure the certification page, including the section for TFA, is signed by the head of agency.
 - d. Verify TFA 2004 documents have been submitted for agencies with contractor access. If TFA 2004 documents have not been submitted for an agency with contractor access, then begin the rejection process.
 - e. Acknowledge receipt of SSR via email response to agency POC and upload acknowledgement email into the case.
- (2) Inventory Analyst must take the following actions:
 - Assign SSR to DES for analysis of the TFA Section 2004 documents within 3 business days in eCase.
 - Assign IRS IT Contractor/ITS for initial analysis within 3 business days in the electronic case management system and move case to Analysis/Preparation.

11.3.36.5.6
(02-24-2025)
SSR Analysis

- (1) SSR reviewers need to have a thorough understanding of applicable statutes, Treasury regulations, agency agreements and contracts, and the agency's and their contractor's systems for processing FTI.
- (2) SSR reviewers will review the SSR for the following:

SSR Reviewer	Actions Taken
DES	<p>Within 15 calendar days of assignment complete the following:</p> <ol style="list-style-type: none">a. Ensure contractor and subcontractor access outlined in SSR Section 3 is IRC 6103 compliant.b. Review agency TFA 2004 contractor worksheet.c. Review information documented on Sections A-G of the TFA 2004 onsite review template.d. Input case notes with standardized language identifying the TFA 2004 Section 2004 review results.

SSR Reviewer	Actions Taken
ITS	<p>Within 20 calendar days of assignment complete the following:</p> <ol style="list-style-type: none"> Conduct a review of the agency's submission (Ex. FL123-DOR-SSR-1231202X.zip) which must include the SSR, SSR signed certification page, and attachments. If the signature page is deficient, the specialist or reviewer must notify the inventory analyst within 5 days of assignment. If the SSR document references attachments that are not present, the specialist or reviewer will notify the inventory analyst within 5 days of assignment. Verify the agency contact information listed in the SSR (e.g., head of agency, title, address, name of agency) against the electronic case management system agency contacts section. Review the DES recommendation in the notes to determine if the agency utilizes contractors or there are additional issues and update the SSR response for Section 3.1.3 with the appropriate standardize response. Review information documented in Section H of the TFA 2004 onsite review template, adding a comment to Section 1 if any findings would result in a Critical finding. Use the SSR processing checklist to review and complete agency's SSR. The checklist is to be completed alongside the review of the SSR with a response for each control/section in the SSR document, inserting comments for each. Ensure that the SSR was submitted on the correct SSR template. Ensure that all information system components listed are under vendor support.

11.3.36.5.7
(02-24-2025)

SSR Processing

- (1) ITS must prepare the approval package for Quality Review (QR) within 20 calendar days of receipt.

- Prepare and upload the transmittal letters to be sent to the agency.
- Prepare and upload the SSR Processing Checklist.
- Complete the SSR analysis and upload the updated SSR to be sent to the agency.

Note: IRS IT Contractors can be assigned SSRs for review of the Computer Security Controls, reference IRM 11.3.36.1.3, Roles and Responsibilities for additional information.

- (2) Update Comments and “Email Notification Comment” under the electronic case management system workspace using the appropriate naming convention.
- (3) Submit case to QR.
 - Cases requiring rework, must be resubmitted to QR with corrections within 3 calendar days.
 - Cases requiring no rework will be submitted for Manager Approval
- (4) Management must conduct approval on SSR cases and review SSR cases from QR within 5 calendar days of assignment.
 - Cases requiring rework, must be resubmitted to QR with corrections within 3 calendar days.
 - Management Assistant will send out documents and release the case if no rework is required.
- (5) All Office of Safeguards employees assigned or processing SSRs are responsible for documenting in case notes any occurrence resulting in missed timeframes.

11.3.36.5.8
(02-24-2025)

Delinquent or

Incomplete Annual SSRs

- (1) Agencies who submit SSRs with incomplete information must be notified through email contact from the Safeguards Mailbox Staff.
- (2) When possible, delinquent SSRs must be resolved through telephone call or email from the Strategic Task Alliance Team (STAT) with the agency POC. STAT procedures are explained in detail under IRM 11.3.36.16.1, Guidelines for Safeguards STAT Enforcement of Safeguard Reporting Requirements.
- (3) Formal procedures to withhold FTI can be initiated if an agency fails to:
 - Send in an acceptable report.
 - Include required evidentiary documentation.

11.3.36.6
(02-24-2025)

**Safeguard Review
Preliminary Findings
Report (PFR)**

- (1) The Preliminary Findings Report (PFR) must be completed and presented to an agency at the conclusion of a Safeguard review. The PFR identifies findings which require correction to improve the safeguarding of FTI in accordance with Publication 1075 .
- (2) For each finding identified, the evaluated risk for potential loss, breach or misuse of FTI establishes the recommended timeframe for its resolution. The risk category is noted next to each finding and the findings are ordered in the report according to priority for resolution to assist the agency in establishing priorities for corrective action.

Risk Category	Associated Time Frame for Resolution
Critical	3 months from the date of the review closing conference
Significant	6 months from the date of the review closing conference
Moderate	9 months from the date of the review closing conference

Risk Category	Associated Time Frame for Resolution
Limited	12 months from the date of the review closing conference

Note: Risk Category associated timeframe for resolution, must not end on a non-workday (i.e. weekend or holiday). If falling on a non-workday, then shift the Risk Category later to the next available workday.

- (3) A preliminary closing is conducted when the review is still in progress because additional locations must be visited or outstanding issues must be resolved. At the conclusion of those activities, the DES must conduct a final review closing conference, generally by conference call. The DES must inform and receive approval from the Chief, SRT/FRT prior to conducting a preliminary closing.
- (4) Safeguard Review PFR Completion of Findings by ITS.
 1. Complete Safeguards Computer Security Evaluation Matrices (SCSEMs) with finding statement for failed tests.
 2. Attach completed SCSEMs to electronic case management system with the information in the following table:

Information	Explanation
Primary Agency	Include the agency code and type Example: MAXXX-CS
Shared Agencies	Include agency codes/types for any applicable shared agencies
Risk Level	Critical, Significant, Moderate, or Limited
SCSEM Type	Technology Type Example: Windows 2003, Network Assessment, etc
PFR Title & Hostname	Document how the system title must be documented on the PFR Example: Windows 7 Tumbleweed Server (WINTWX01)

3. Complete the Section H Critical findings by including the hostname and reason for the Critical Risk, or if no findings use state "No critical findings identified".
4. Complete Section H of the PFR template by identifying the number of systems including the host names as a weighted Pass Rate Percentage and list at least two areas of notable risk in bullet format.

5. Compile technologies and use the following order when applicable starting with the MOT Assessment, Network Assessment, or system including the hostname.
6. Section H of the PFR must be submitted to the DES no later than 2 hours prior to the scheduled agency closing conference with any deviation from that timeframe requiring approval by the Chief, SRT/FRT.

Note: IRS IT Contractors can be assigned to Safeguard Reviews and assist with completion of the PFR findings, reference IRM 11.3.36.1.3, Roles and Responsibilities for additional information.

- (5) Safeguard Review PFR completion by the DES with the information in the following table:

Step	PFR Completion Procedures
1	The DES must use the most current PFR report template from the Office of Safeguards SharePoint <i>Job Resources and Reference Documents</i> .
2	The DES must keep track of all findings during the onsite safeguard review and has discretion to determine the process for tracking the findings throughout the onsite review.
3	As findings are identified during the onsite safeguard review the DES and IRS IT contractor/ITS must discuss the findings with the agency POCs (physical and IT) providing recommendations for mitigation. If possible, the DES must review the findings with the agency's Primary POC prior to the closing conference.
4	Input the findings in the appropriate Section A - G in order by risk category beginning with the highest level risk. Example: All Critical findings, all Significant findings, all Moderate findings, and all Limited findings within each section.
5	The risk category is listed immediately following the finding in parenthesis. Example: The agency fails to maintain a system of records (logs) identifying the date information was received, its exact location, who has access to data and, if disposed, the date and method of disposition. See Publication 1075 Section 3.2 and Exhibit 9. (Significant)
6	Include a comment after each finding in parenthesis that briefly describes the issue. Example: The FTI reports electronically sent to the field offices are not logged.

Step	PFR Completion Procedures
7	Add the mandatory comments as required on the PFR for the agency type.
8	The DES must combine the Section H with the Section A - G portion of the PFR to provide a complete document to the agency. The lead IRS IT Contractor/ITS must be available to assist and/or combine the documents in this process if the DES encounters difficulties.
9	Provide the completed PFR to the agency Primary POC prior to the closing conference. The lead IRS IT Contractor/ITS must be available to assist in this process should the DES encounter difficulties to ensure that the closing goes forward as scheduled. The document must be provided in enough time to allow the agency Primary POC to make enough copies prior to the closing conference. The DES will advise the agency Primary POC of the number of copies needed for IRS staff and contractors, if applicable.

- (6) Post Safeguard Review (Closing Conference held) PFR Submission.
 - a. DES must upload a copy of the PFR to into the electronic case management system no later than the two business days following the review closing conference.
 - b. Notify the SRT/FRT MA the PFR was uploaded and date of the closing conference.
- (7) Preliminary Closing Conferences – Procedures to be followed if you were unable to complete the review and a preliminary closing has been approved:
 - a. Complete the Outstanding Items at the Time of the Closing Conference page (last page of report).
 - b. Schedule with the agency Primary POC a future date/time for a call to conduct the closing conference and apprise the Chief, SRT/FRT. The subsequent closing conference must be scheduled, if possible, within one week of the onsite review.
 - c. Once the outstanding issues have been resolved, the PFR must be updated. Refer to paragraphs (4) and (5) above.
- (8) When the official closing of the review has occurred the DES must upload the PFR into the electronic case management system.

11.3.36.7
(02-24-2025)
**Safeguard Review
Reports (SRR)**

- (1) The SRR is the final report and serves as a record of the IRS's evaluation of an agency's compliance with the safeguard requirements for the protection of tax returns or return information as prescribed in IRC 6103(p)(4).
- (2) The requirements in the IRC have been augmented by other Treasury Department or IRS requirements as well as NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*; these requirements must be addressed as well.

Example: NIST SP 800-53 mandates that all automated information systems and networks which process, store, or transmit sensitive but unclassified

(SBU) information are to meet the requirements for Management Security Controls, Operational Security Controls and Technical Security Controls.

- (3) Treasury's and NIST SP 800-53 requirements have been incorporated in IRS Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies* as requirements for recipient agencies.
- (4) It is important that a SRR document all actions agencies and/or authorized contractors must take to achieve compliance with FTI safeguards.
- (5) The report must be a complete document that provides a description of all findings and recommended corrective actions. Reports must adhere to the Office of Safeguards reporting guidelines.
- (6) All SRRs will be prepared according to a standard format to ensure all reviews and reports address the key areas of the IRS's safeguard requirements. SRR templates can be located on the Office of Safeguards SharePoint *Job Resources and Reference Documents*.
- (7) The report must be transmitted to the agency with the most current SRR cover letter located on the Office of Safeguards SharePoint *Job Resources and Reference Documents*.
- (8) All safeguard reviews must address the adequacy of computer security. The report must contain a review of the agency's and contractor's compliance with the computer security requirements contained in the most current version of IRS Publication 1075.
- (9) The CAP accompanies the report and is used by the agency to respond to the SRR and the Office of Safeguards to track the agency's progress. The agency will report actions taken on safeguard review recommendations that are outstanding in their semi-annual CAP. Refer to Publication 1075, Section 2.E.5.1, CAP Submission Instructions for further guidance.
- (10) All actions taken and pertinent information regarding the entire review process and the report must be clearly outlined in the notes of the SRR case.
- (11) The Office of Safeguards standardized findings language must be used to assist in preparing quality reports using a standard format that will improve consistency, accuracy, and the quality of reports issued to the agency partners. Safeguards Standardized Language can be located on the Office of Safeguards SharePoint *Job Resources and Reference Documents*.
- (12) Timeliness of Reports - SRR must be issued to the agency within 45 days of the final closing conference to convey our commitment to ensuring the confidentiality of the FTI. Management must be apprised of circumstances involving reports that have not been forwarded timely.

Note: A review is completed when the SRR is issued to the agency.

- (13) MAs will create a case on the electronic case management system and hold it in "Intake" status until it is ready for "Analysis/Prep". The DES will send the MA an email indicating the PFR had been uploaded and request the case be updated to "Analysis/Prep" status. The SRR case will show in the DES "Inbox"

on the electronic case management system. Reference the eCase User Guides for information on creating cases and uploading documents.

- (14) A SRR is issued even if there is no agreement with the agency on all findings and/or recommendations. The IRS and the agency will continue in a cooperative effort to ensure that the FTI is adequately protected from unauthorized access or disclosure.
- (15) Safeguards Staff must reference IRM 11.3.36.4, Documentation and IRM 11.3.36.1.7, Related Resources for additional information on working SRRs.

11.3.36.7.1
(02-24-2025)
SRR Content

- (1) **INTRODUCTION** – The DES must use the most current template based on the type of agency reviewed. Verify that the Introduction matches the code authority for which the agency is receiving information. For federal agencies, briefly outline the statutory provisions, in general, which permit the disclosure of returns or return information, and the intended purpose or benefit(s) of the disclosures. Any limitations or restrictions imposed by the IRC or regulation can be included in the introduction portion of the report.
- (2) **BACKGROUND** – This section, which is agency and contractor specific, must contain the name of the agency reviewed, and if applicable, the specific organization(s) or function(s) reviewed within that agency. If several, separate, programs are being reviewed, the background section must give a brief description of each program.

- Insert the information highlighted in red in the SRR template.
- For HS and CS agencies you must identify the relationship between the field office/county offices and the state.

Example: state run/county administered or state run/state administered

- In the contractor portion you must develop a comprehensive list of all contractors that are used for services that involve the disclosure of FTI (MM-DD-YYYY). Exhibit 7 Contract language must be addressed for each contractor, unless all contracts either contain or do not contain the language then a blanket statement can be used for all.

Example: ABC Company – manages XYZ Data Center that houses FTI in production and networking technologies. The contract contains the required safeguard language. If the contract does not contain the required safeguard language add the following language: The contract does not contain the required safeguard language. Refer to finding C.# of this report for further discussion of required corrective actions.

- In the IT portion you must develop a description of how the agency's IT services are provided. If the agency uses an embedded IT as well as a consolidated data center, the services that each provides to the agency must be clear. The Service Level Agreement (SLA) or contract with the agency providing the IT services must be addressed. The last sentence of the IT paragraph must state who at the agency will be required to address the Section H findings.

Example: XDOR information technology services are provided by an embedded staff which provides application support for their Collection System (XDORCS) application that manages

taxpayer accounts and contains FTI. XDOT is a separate state agency managing a consolidated data center and supporting several agencies. ABC Inc. manages the XDOT disaster recovery site. XDOT provides all other information technology services and support for XDOR including procurement and maintenance of hardware and software, telecommunications and networking services, infrastructure services, help desk functions, server and workstation provisioning, perimeter security, and monitoring for the systems that XDOR uses to receive, process, store, and access FTI. The SLA between XDOR and XDOT contains the required safeguard language. The computer security findings in Section H will require corrective action by XDOR and XDOT.

- (3) **SCOPE** – This section contains descriptive reviewer information regarding the conduct of the review. This section of the report must give the reader a sense of how the review was conducted and what programs and procedures were included or excluded from the review. In addition, the scope and objectives section must also indicate:
- a. The highlighted information in red from the template.
 - b. Correct spelling of reviewers names.
 - c. Correct dates of review.
 - d. Government Liaison (GL) participation in the review must be noted, if applicable.
 - e. Agency POC listed as coordinating the review and their title.
 - f. In the locations section, list every location that was visited for your agency. If someone else visited a location for you, it must be listed and annotated who visited the site.
 - g. In the personnel section, list everyone interviewed and their title, including personnel involved in the Section H review.
- (4) **FINDINGS AND RECOMMENDATIONS** – All safeguard review reports will address identified deficiencies for each requirement enumerated in IRC 6103(p)(4), and other requirements determined to be necessary to ensure the confidentiality of FTI and return information. To ensure that all the requirements of the IRC, Publication 1075, and the IRM have been addressed, Sections A - H subsections will contain a statement of the requirement, followed by a description and discussion of the findings and recommendations.

Note: When an SRR is generated from the electronic case management system the Findings and Recommendations must be copied to the most current version of the SRR template before updates to the Title page or Cover Sheet, Table of Contents, Acronym Listing, Introduction, Background and Scope are completed.

11.3.36.7.2
(02-24-2025)
**SRR Processing
Procedures**

- (1) DES must enter Section A - G findings identified from the review into eCase. Supplementary guidance for the automatic upload can be located in the eCase User Guides on the Office of Safeguards SharePoint *Job Resources and Reference Documents*.
- (2) The DES must import all Section H Parent Findings and Component Findings from the document loaded to the electronic case management system by the IRS IT Contractor/ITS within 20 calendar days of the closing conference, using

the electronic case management system “SFG Finding Import” tool. Parent Findings and Component Findings will be created for every Section H finding even if only one component exists. Supplementary guidance for the automatic upload can be located in the eCase User Guides on the Office of Safeguards SharePoint *Job Resources and Reference Documents*.

- (3) DES must complete the SRR using the most current SRR template.
 - a. Generate findings for the report from the electronic case management system once all findings have been added to the electronic case management system. Supplementary guidance generating the report findings can be located in the eCase User Guides on the Office of Safeguards SharePoint *Job Resources and Reference Documents*.
 - b. Validate the findings in the generated SRR match the findings entered in the SRR case.
 - c. Copy the generated findings into the most current SRR template which includes information from the Title page or Cover Sheet, TOC, Acronym Listing, Introduction, Background and Scope
- (4) DES must prepare the SRR Letter using the most current template available.
- (5) ITS must upload the documents associated with the Section H to the case using the correct naming convention for all documents.
 - a. Preliminary Security Evaluation (PSE) document
 - b. SCSEM
 - c. Critical Response Analysis (if applicable)
 - d. Section H spreadsheet for import to eCase
 - e. Section H Introduction document that includes the Management Operational and Technical (MOT) Controls and Technology headers along with agency responses and IRS comments for Critical findings

Note: IRS IT contractors can be assigned to conduct Safeguard Reviews and be responsible for uploading documents. Reference IRM 11.3.36.1.3, Roles and Responsibilities for additional information. Final documents must be free of spelling and grammar mistakes and must not be encrypted.

- (6) DES must upload safeguard review documents using the correct naming convention for all documents.
 - a. Agency Contact Information (ACI) Sheet
 - b. Review Prep Questionnaire (RPQ)
 - c. Safeguards Disclosure Security Evaluation Matrix (SDSEM)
 - d. Critical Response Analysis (if applicable)
 - e. Review Preparation Check List
 - f. Final Agenda
 - g. Preliminary Findings Report
 - h. Safeguard Review Report
 - i. Safeguard Review Report Letter
 - j. Completed SRR DES Checklist
- (7) DES must close out all findings from the previous review. This includes all Section H component findings. Make a case note in the previous SRR case as well as the current SRR case stating the reason for closing the findings (due to a new review).

- (8) DES must update Comments and “Email Notification Comment” under the electronic case management system workspace.
- (9) DES must submit case to Quality Review within 30 calendar days of the Closing Conference.
 - Cases requiring rework, must be resubmitted to QR with corrections within 3 calendar days.
 - Cases requiring no rework must be submitted for Manager Approval.
- (10) Management must conduct approval on SRR cases and review SRR cases from QR within 5 calendar days of assignment.
 - Cases requiring rework, must be resubmitted to QR with corrections within 3 calendar days.
 - Management Assistant will send out documents and release the case if no rework is required
- (11) SRRs are considered timely if the case, is released within 45 calendar days of the closing conference. All Office of Safeguards employees assigned or processing SRRs are responsible for documenting in case notes any occurrence resulting in missed timeframes.

11.3.36.8
(02-24-2025)
**Corrective Action Plan
(CAP)**

- (1) The CAP is the report that contains the findings, the recommendations and the targeted implementation dates for items identified for corrective action during an on-site, remote or hybrid review. The CAP document has functionality that allows the agencies to report their progress on any corrective actions; the IRS provides the agency a SRR along with a CAP upon completion of any review.
- (2) The agency must update and submit the CAP semi-annually to document all corrective actions, both taken or planned, in response to the findings enumerated in the SRR. CAP Submission Instructions along with the CAP Submission Dates are located in Publication 1075 Section 2.E.5.2, CAP Submission Dates.
- (3) If the SRR was issued within 60 days from the upcoming CAP due date, in the chart located in Publication 1075 Section 2.E.5.2, CAP Submission Dates, the agency’s first CAP will be due on the subsequent reporting date to allow the agency adequate time to document all corrective actions proposed and taken. Agency CAP submissions provided to the Office of Safeguards within 60 days of an upcoming review will be responded to as part of the review process. Agencies can request a CAP extension when extenuating circumstances exist, for no more than 30 calendar days. Extension requests must be sent to the Office of Safeguards via Secure Data Transfer (SDT) or through the *Safeguards Mailbox* with the subject **CAP Extension Request**.
- (4) Once the agency has submitted their semi-annual CAP for review and response from the Office of Safeguards; it is the responsibility of the Mailbox Staff; Inventory Analysts; ITS; Disclosure Enforcement Specialists; SRT/FRT Chiefs; and SRT Management Assistants to follow the CAP SOPs and CAP Paragraph Guidance to process, respond timely, and return the agency CAP.
- (5) Safeguards Staff must reference IRM 11.3.36.4, Documentation and IRM 11.3.36.1.7, Related Resources for additional information on working CAPs.

11.3.36.8.1
(02-24-2025)
CAP Assignment

- (1) Mailbox staff must do the following when a CAP is received in the mailbox:
 - a. Retrieve the CAP and create a case in the electronic case management system within 3 business days from mailbox receipt.
 - b. Upload the agency CAP into the case and upload responses into "Related Case" SRR.

Note: Attachments in the electronic case management system must not be password protected.

 - c. Acknowledge receipt of CAP via email response to agency POC and upload acknowledgement email into the case.
- (2) Inventory Analyst must verify the agency is not scheduled for an upcoming safeguard review within 60 calendar days of the CAP received date and email the DES and IT Contractor/ITS to inform them of the upcoming Safeguard Review.

Note: This does not apply to agencies that request an extension.

- (3) Inventory Analyst must assign the following:
 - a. Section A-G CAP responses to DES as "Case Owner" and Analyst within 3 business days of receipt.
 - b. Section H to IRS IT Contractor or ITS as "Analyst" within 3 business days of receipt.
- (4) Inventory Analyst must review Section H to validate open findings and if all findings have been closed, then email IT Contractor or ITS to advise Section H review is not required.

11.3.36.8.2
(02-24-2025)
CAP Analysis

- (1) CAP reviewers need to have a thorough understanding of applicable statutes, Treasury regulations, agency agreements and contracts, and the agency's and their contractor's systems for processing FTI.
- (2) Assigned individuals must conduct an initial review of the CAP submission and acknowledge receipt of CAP by updating notes in the electronic case management system within 10 calendar days for the following:

If ...	Then ...
Additional coordination is needed from Office of Safeguards personnel.	Contact the mailbox within the initial 10 calendar day timeframe to secure any attachments or information not uploaded to the case.
Additional coordination is needed from the agency.	Contact the agency within the initial 10 calendar day timeframe to secure missing attachments or clarify additional information is needed.

If ...	Then ...
Additional information is required from the agency.	Send a detailed email requesting the additional information and allow 5 business days for the agency to respond.

- (3) Assigned individuals must verify the agency is not scheduled for an upcoming Safeguard review within 60 days of CAP received date.
- (4) If ITS is assigned, then ITS must update Section H of the CAP using the following steps based on an evaluation of the information provided by the agency:

Step	Evaluation
1	Validate evidentiary documentation was provided, as applicable (Significant and Critical findings require evidentiary documentation to be provided).
2	Appropriately close Component and Parent Findings, if appropriate (all areas described in finding and discussion must be addressed and be sufficient to close findings).
3	Update the Finding Status (open, closed-verification provided or closed-no verification required).
4	Update the Actual Closure Date appropriately (Closure date must be updated to date provided by agency or date the CAP was received, but cannot be prior to the Finding Initialization Date).
5	Prepare IRS Comments which reflects correct language and satisfactorily addresses Agency Response.
6	ITS must complete analysis of Section H and update of Component and Parent Findings within 20 calendar days of receipt.

Note: IRS IT Contractors can be assigned CAPs for Section H analysis and update, reference IRM 11.3.36.1.3, Roles and Responsibilities for additional information.

- (5) DES must update Section A-G of the CAP using the following steps based on an evaluation of the information provided by the agency:

Step	Evaluation
1	Validate evidentiary documentation was provided, as applicable (Significant and Critical findings require evidentiary documentation to be provided).

Step	Evaluation
2	Appropriately close Parent Findings, if appropriate (all areas described in finding and discussion must be addressed and be sufficient to close finding).
3	Update the Finding Status (open, closed-verification provided or closed-no verification required).
4	Update the Actual Closure Date appropriately (Closure date must be updated to date provided by agency or date the CAP was received, but cannot be prior to the Finding Initialization Date).
5	Elevate Critical and Significant findings to SRT/FRT Chief if agency indicates they will not be corrected and provides no plan for remediation.
6	Prepare IRS Comments which reflect correct language and satisfactorily addresses Agency Response.

11.3.36.8.3
(02-24-2025)
CAP Processing

- (1) DES must prepare and upload the following documents for a management approval package:

- Appropriate CAP letters using the appropriate naming convention format.

If ...	Then ...
Scheduled for a Safeguard review within 60 days	Prepare Letter 6059 and Letter 6056
Section A-H Findings remain open	Prepare Letter 6070 and Letter 6075
Section A-H Findings have been closed	Prepare Letter 6046 and Letter 6055

- Additional information provided by agency, if applicable.
 - The completed DES CAP Checklist.
- (2) CAPs must be forwarded for Management Approval within 30 calendar days of receipt.
- (3) Update Comments and “Email Notification Comment” under the electronic case management system workspace using the appropriate naming convention.
- (4) DES must update case status to “Quality Review”.
- (5) QR will not review the case but must update the case status to “Management Approval”.
- (6) Management must conduct approval on CAP cases within 5 calendar days of assignment.

- Cases requiring rework, must be resubmitted to QR with corrections within 3 calendar days.
- Management Assistant will send out documents and release the case if no rework is required.

(7) CAPs are considered timely if the case, is released within 45 calendar days of receipt. All Office of Safeguards employees assigned or processing CAPs are responsible for documenting in case notes any occurrence resulting in missed timeframes.

11.3.36.9
(02-24-2025)
Technical Inquires (TI)

- (1) TIs are communications routed through the *Safeguards Mailbox* requesting assistance with interpretations of Publication 1075 or other routine safeguarding matters.
- (2) The objective of the TI process is to provide prompt, accurate answers to agency inquiries on the proper safeguarding of FTI in accordance with Publication 1075 and the application of existing Office of Safeguards guidance.

Example: Security and Privacy Alerts

- (3) TIs received directly by Office of Safeguards staff, either verbally or via email, must be forwarded to the *Safeguards Mailbox*, for processing. TIs received directly by Government Liaison Disclosure Safeguards (GLDS) staff, either verbally or via email, must be returned to the requestor for direct submission to the *Safeguards Mailbox*. See IRM 11.3.36.9.2, TI Analysis for instances that do not qualify as a TI.
- (4) TI responses must be brief and direct, specifically addressing the agency's inquiry and clearly state current IRS Office of Safeguards policy to close the matter and avoid on-going discussions on the same issue.
- (5) Safeguards Staff must reference IRM 11.3.36.4, Documentation and IRM 11.3.36.1.7, Related Resources for additional information on working TIs.

11.3.36.9.1
(02-24-2025)
TI Assignment

- (1) Mailbox staff must do the following when a TI is received in the mailbox:
- a. Retrieve the TI and create a case in the electronic case management system within 3 business days from mailbox receipt.
 - b. Upload the agency TI into the case.
 - c. Acknowledge receipt of TI via email response to agency POC and upload acknowledgement email into case.
- (2) Generally, an inventory analyst will assign the following types of TIs to a DES within 3 business days from mailbox receipt:
- Clarification of physical security requirements in Publication 1075 and statute related questions.
 - CAP questions relative to SRR Section's A - G findings.
 - Questions relative to TFA 2004.
- (3) Generally ITS or the IRS IT Contractor will be assigned the following types of Technical Inquires within 3 business days from mailbox receipt:
- Clarification of computer security requirements in Publication 1075 .
 - CAP questions relative to SRR Section H findings.
 - SCSEM questions.

- Vulnerability scanning questions.
- SSR Questions.

- (4) Generally, physical security TIs from agencies under an open review must be assigned to the DES conducting the review.

11.3.36.9.2
(02-24-2025)
TI Analysis

- (1) TI reviewers need to have a thorough understanding of applicable statutes, Treasury regulations, agency agreements and contracts, and the agency's and their contractor's systems for processing FTI. Research and contact other Office of Safeguards personnel (e.g., Senior DES, SRT/FRT Chief, TA) as needed.
- (2) TI reviewers must conduct an initial review of the TI to determine if the TI is an issue that is not covered in Publication 1075, is not a Safeguards issue, or requires additional case actions. Use the following table to determine the appropriate action:

If ...	Then ...
Additional information is required from the agency.	Send a detailed email requesting the additional information and allow 5 business days for the agency to respond.
The case requires additional IRS IT Contractor or ITS assignment.	IT support can be coordinated through a government employee's Chief or through the Review Technical Advisor Team.
Involvement by another department is necessary or required (e.g., SOI).	Forward the information for coordination.
TI is not an Office of Safeguards issue or does not pertain to the safeguard program.	Provide a telephonic or email explanation to the agency that the Safeguards purview is limited to Publication 1075 requirements. If applicable, refer the question to the appropriate GLDS function.
TI is from an entity not subject to Office of Safeguards oversight or is not a partner agency.	Provide a telephonic or email explanation to the requester that TIs must be submitted by agencies with a current agreement to receive FTI directly from IRS or obtains FTI through an authorized secondary source (e.g., SSA, OCSE, BFS, CMS).

If ...	Then ...
TI is requesting information on how other agencies implement security requirements.	Provide a telephonic or email explanation to the agency that the Safeguards purview is limited to Publication 1075 requirements. If applicable, provide a response in accordance with Publication 1075 or the application of existing Office of Safeguards guidance.

- (3) Upload any emails sent requesting additional information from agency, IT Contractor/ITS assignment or requests for coordination.
- (4) If a timely response is not received for additional information, the TI will be closed with an email advising the agency of closure and explaining:
 - What information is required to answer the question, and
 - The TI can be resubmitted with the required information for processing/ response.

11.3.36.9.3
(02-24-2025)
**TI Processing
Procedures**

- (1) TI reviewers must prepare an appropriate response for resolution by telephone or in writing:

Response Type	Action Taken
Telephonic Resolution	<p>Contact the requestor and resolve the inquiry during the initial phone discussion.</p> <ol style="list-style-type: none"> a. If the inquiry requires IT resources, facilitate discussion with the inquirer in coordination with necessary IRS personnel. b. Document the discussion and answer provided to the agency in eCase. c. Provide a follow-up written response to the agency if needed or requested. d. Case notes must document all research conducted and/or guidance provided by other IRS personnel and include a brief summary of the response provided to the agency.

Response Type	Action Taken
Written Response	<p>Prepare written response on the Safeguards receipt acknowledgement email to the original incoming inquiry uploaded to the electronic case management system in the appropriate format.</p> <ol style="list-style-type: none"> Include intervening email threads in the written response. Include all attachments to be sent to the agency as part of the written response, if applicable. The response must be concise and appropriately respond to the agency question(s). Email responses must follow the format below. Cite Publication 1075 references as appropriate. The response must provide guidance that is complete but does not simply restate Publication 1075 text.

(2) Written responses to TIs must follow the following format:

TI Response Email Format	TI Response Email Example
Opening: Hello [TI Submitters First Name and Last Name]	Hello John Doe,
Introduction: This is in response to your inquiry dated [Month DD, YYYY], concerning [State the subject]	This is in response to your inquiry dated May 27, 2022, concerning the record retention period for Federal tax information (FTI).

TI Response Email Format	TI Response Email Example
Type narrative response	The Publication 1075 reference to the requirements to retain records for a period of five (5) years is referring to the record keeping requirements that require tracking the receipt of records through destruction. These records must be maintained for five (5) years or the agency's applicable records control schedule must be followed, whichever is longer. Agency can maintain FTI as long as the FTI is needed by the agency and is used in accordance with the Internal Revenue Code and the Federal/State agreement(s) with the agency. The requirement of agencies is that the FTI be destroyed when it is no longer needed or used. Agencies are required to establish a records control schedule to ensure the disposal of FTI is done on a routine basis and in accordance with Publication 1075.
Cite Publication 1075 references as appropriate	For further information, please refer to Publication 1075, Section 2.4 and 3.1.
Include contact information	If you have any further questions about this matter, please refer them to Disclosure Enforcement Specialist, DES name at DES telephone number or at DES email address. I hope this fully responds to your inquiry. <i>SafeguardReports@irs.gov</i> . I hope this fully responds to your inquiry.

- (3) Ensure the agency will fully meet Publication 1075 standards on the issue.
- (4) All TIs do not require an email/written response. Utilize the most appropriate method for the type of issues/inquires raised.
- (5) DES or ITS must prepare and upload the following documents for a management approval package:
 - a. The original agency TI (this should already be uploaded by Mailbox staff when the case was created)
 - b. Additional information provided by agency, if applicable

- c. Written TI Response or withdrawal email, if applicable
- d. DES TI Checklist located on the Office of Safeguards SharePoint *Job Resources and Reference Documents*

Note: IRS IT Contractors can be assigned TIs to address inquiries involving Publication 1075 Computer Security Controls, reference IRM 11.3.36.1.3, Roles and Responsibilities.

- (6) Update Comments and “Email Notification Comment” under the electronic case management system workspace using the appropriate naming convention.
- (7) Assigned employees must forward case to QR or Management Approval within 20 calendar days of receipt.
- (8) Submit cases with the following issue codes to Quality Review:

Code Group	Issue Code
A – Record Keeping	A1, A2, A3, A4, A5
B – Secure Storage	B1, B2, B3, B4, B17
C – Restricting Access	C1, C2, C3, C4, C5, C6, C7, C8, C9, C11, C14, C15, C16, C25, C26
D – Other Safeguards	D1, D2, D3, D4
E – Reporting Requirements	E6, E7
G – Need and Use	G1, G2
H – Section H	All

- Cases with issue codes not listed in the table above can be forwarded for Manager Approval by QR without review.
 - Cases requiring rework, must be resubmitted to QR with corrections within 3 calendar days.
 - Cases requiring no rework will be submitted for Manager Approval.
- (9) Management must conduct approval on TI cases and review TI cases from quality review within 5 calendar days of assignment.
 - a. Cases requiring rework, must be resubmitted to QR with corrections within 3 calendar days.
 - b. Management Assistant will send out documents and release the case if no rework is required.
 - (10) TIs are considered timely if the case, is released within 30 calendar days of receipt. All Office of Safeguards employees assigned or processing TIs are responsible for documenting in case notes any occurrence resulting in missed timeframes.

11.3.36.10
(02-24-2025)
45 Day Notifications

- (1) Publication 1075 requires agencies to notify the Office of Safeguards prior to executing any agreement to disclose FTI to a contractor, no less than 45 days prior to the disclosure of FTI.
- (2) In addition to the disclosure of FTI to a contractor, the following circumstances or technology implementations also require the agency to submit notification to the Office of Safeguards via the *Safeguards Mailbox*, no less than 45 days ahead of the planned implementation:

Activities that involve FTI	Response
Cloud computing	Notification to the Office of Safeguards.
Disclosure to a contractor	Notification to the Office of Safeguards, but only applicable for agencies specifically authorized pursuant to IRC 6103 statute or regulation.
Re-disclosure by contractor to subcontractor	Advanced approval is required to proceed from the Office of Safeguards, but only applicable for agencies specifically authorized pursuant to IRC 6103 statute or regulation.
Tax modeling for tax administration	Advanced approval is required to proceed from the Office of Safeguards.
Test environment	Advanced approval is required to proceed from the Office of Safeguards.

- (3) The agency is required to provide notification which includes all of the information requested in Exhibit 6 of Publication 1075.
- (4) Safeguards Staff must reference IRM 11.3.36.4, Documentation and IRM 11.3.36.1.7, Related Resources for additional information on working 45 Day Notifications.

11.3.36.10.1
(02-24-2025)
**Agency Submission of
45 Day Notification and
Correspondence**

- (1) All correspondence must be sent electronically by Secure Data Transfer or encrypted using SecureZip, to the *Safeguards Mailbox* and include a cover letter signed by the head of the agency or authorized delegate.
- (2) Use of templates specified in Publication 1075 will enhance the agency's ability to provide all of the information to process the notification and will minimize processing errors.

11.3.36.10.2
(02-24-2025)
**Notification
Assignments**

- (1) Mailbox staff must do the following when a 45 Day Notification is received in the mailbox:

- a. Retrieve the 45 Day Notification and create a case in the electronic case management system within 3 business days from mailbox receipt.
 - b. Upload the agency 45 Day Notification into the case.
 - c. Acknowledge receipt of 45 Day Notification via email response to agency POC and upload acknowledgement email into case.
- (2) Mailbox Staff must assign 45 Day Notification Letters for contractor and/or sub-contractor access to FTI to a DES as “Case Responsible” and “Analyst” within 3 business days from mailbox receipt.
- (3) Mailbox Staff must assign 45 Day Notification Letters for Live Data Testing and Cloud Computing that require IT review within 3 business days from mailbox receipt as follows:
 - IRS IT Contractor/ITS as “Case Responsible” in eCase.
 - DES as “Analyst” in eCase.
- (4) Inventory Staff periodically review inventory and can reassign cases, as needed, to ensure inventory is evenly assigned.

11.3.36.10.3
(02-24-2025)
**45 Day Notification
Analysis**

- (1) Within 10 calendar days of case assignment employees assigned 45 Day Notifications must:
 - a. Review the entire notification to confirm proper submission and it contains all required information.

Note: This includes Cloud Computing, Tax Modeling, and Live Data Testing requests.
 - b. If additional information is required from the agency, then send a detailed email requesting the additional information and allow 5 business days for the agency to respond.
 - c. If case requires additional CSR assignment contact S&RT Inventory Analysts to have one assigned.
 - d. Determine if involvement by another department is necessary or required (e.g., SOI) and forward the information for coordination/approval.
 - e. Upload any emails sent requesting additional information from agency, IRS IT Contractor/ITS assignment, or requests for coordination.
- (2) Notifications must be submitted by the agency. If the Office of Safeguards is in receipt of a 45 Day Notification from a contractor or consolidated IT, then request the agency submit the 45 Day Notification. Close the 45 Day Notification case in the electronic case management system using the non-processible template located under the Office of Safeguards SharePoint *Job Resources and Reference Documents*. A new 45 Day Notification case will be opened in the electronic case management system upon receipt of the appropriate 45 Day Notification from the agency.
- (3) Notifications can be withdrawn by the agency. If the Office of Safeguards is in receipt of a withdrawal request, then send an email to the agency acknowledging the withdrawal request and upload to “Attachments” on eCase.
- (4) Review the information provided to ensure it adheres to the standards in Publication 1075 and all Exhibit 6 information was provided. The following table provides information on what analysis is required for each type of 45 Day Notification:

Type of 45 Day Notification	Analysis
Disclosure to a contractor and Re-disclosure by contractor to subcontractors.	DES must utilize the 45 Day Notification Processing Check Sheet located on the Office of Safeguards SharePoint <i>Job Resources and Reference Documents</i> to document notifications adherence to IRC 6103, Publication 1075, and all Exhibit 6 information.
Notifications Involving Tax Modeling, Revenue Forecasting, or Statistical Analysis (Requires coordination with Statistics of Income (SOI))	<ul style="list-style-type: none"> a. Provide SOI a copy of the agency's notification. b. Provide SOI a copy of the agency's current Need and Use document. If no current Need and Use document is on file, obtain a signed copy from the agency and email to the Disclosure Manager for approval. c. Provide SOI a copy of the agency's statement detailing the methodology and data to be used by the contractor. d. DES must utilize the 45 Day Processing Notification Check Sheet located on the Office of Safeguards SharePoint <i>Job Resources and Reference Documents</i> to document notifications adherence to IRC 6103, Publication 1075, and all Exhibit 6 information. e. Incorporate SOI's statement in the closing letter template.

Type of 45 Day Notification	Analysis
Notifications Involving Live Data Testing and Cloud Computing	<ol style="list-style-type: none"> a. ITS must complete analysis of the computer security controls emailing DES and uploading the document analysis within 20 calendar days of receipt. b. DES must utilize the 45 Day Notification Processing Check Sheet located on the Office of Safeguards Share-Point <i>Job Resources and Reference Documents</i> to document notifications adherence to IRC 6103 , Publication 1075 , and all Exhibit 6 information.

Note: IRS IT Contractors can be assigned Notifications to conduct an analysis of the Publication 1075, Computer Security Controls, reference IRM 11.3.36.1.3, Roles and Responsibilities for additional information.

- (5) If the agency fails to appropriately respond by the due date issued, then prepare the non-processible letter located on the Office of Safeguards Share-Point *Job Resources and Reference Documents*.
- (6) Document all information received from the agency in the electronic case management system case Notes and upload documents and emails to the electronic case management system as appropriate.

11.3.36.10.4
(02-24-2025)
**45 Day Notification
Processing**

- (1) DES must prepare and upload the following documents for a management approval package using the appropriate naming convention format.
 - The original agency notification (this should already be uploaded by Mailbox staff when the case was created)
 - Additional information provided by agency, if applicable
 - Closing letter or withdrawal email
 - Completed 45 Day Notification Processing Check Sheet
 - Completed 45 Day Notification Checklist
- (2) Closing letter templates can be accessed on the Office of Safeguards Share-Point *Job Resources and Reference Documents*.
- (3) 45 Day Notifications must be forwarded for QR or Management Approval within 20 calendar days of receipt.
- (4) Update Comments and "Email Notification Comment" under the electronic case management system workspace using the appropriate naming convention format.
- (5) DES must submit cases to QR which meets criteria under IRM 11.3.36.11.4, QR of 45 Day Notifications or have QR forward all other 45 Day Notifications, without review, for Manager Approval.

- Cases requiring rework, must be resubmitted to QR with corrections within 3 calendar days.
 - Cases requiring no rework must be submitted for Manager Approval.
- (6) Management must conduct approval on 45 Day Notification cases and review 45 Day Notification cases from QR within 5 calendar days of assignment.
- a. Cases requiring rework, must be resubmitted to QR with corrections within 3 calendar days.
 - b. Management Assistant will send out documents and release the case if no rework is required.
- (7) 45 Day Notifications are considered timely if the case, is released within 30 calendar days of receipt. All Office of Safeguards employees assigned or processing 45 Day Notifications are required to document in case notes any occurrence resulting in missed timeframes.

11.3.36.11
(02-24-2025)
Quality Review

- (1) The QR process ensures workstream product completeness and adherence to policies and procedures. QR is used to check if all objectives of a quality standard have been achieved. The QR process verifies the following:
- **Finding/ Recommendation Accuracy:** providing the correct finding that describes the agency issue with the correct recommendation/resolution.
 - **Statutory/Regulatory/Publication 1075 Accuracy:** adhering to statutory/regulatory and Publication 1075 requirements when preparing reports/responses to partner agencies.
 - **Process/Procedural Accuracy:** adhering to non-statutory/non-regulatory internal and Publication 1075 requirements when preparing reports/responses to partner agencies.
 - **Professionalism:** promoting a positive image of the IRS by using effective communication techniques.
 - **Timeliness:** submitting reports/responses in a timely manner through the use of proper workload management and time utilization techniques.
 - **Documentation:** All steps taken in the review process must be documented within three business days unless extenuating circumstances require additional time. All notes, worksheets, communication contacts, memoranda, and other correspondence must be retained in the file and in notes on the electronic case management system to support decisions.
- (2) Safeguards Staff must reference IRM 11.3.36.4, Documentation and IRM 11.3.36.1.3, Related Resources for additional information on working cases for QR.
- (3) QR is conducted for the following case types:
- a. SSRs
 - b. SRRs
 - c. TIs
 - d. 45 Day Notifications

Note: As part of QR, ITS must conduct a quality control review of IRS IT Contractor work on SSRs, TIs, and 45 Day Notifications.

11.3.36.11.1
(02-24-2025)

**Quality Review of
Safeguard Security
Reports**

- (1) The following documents must be uploaded in the electronic case management system when the Quality Reviewer receives the case file. Each of these documents must be reviewed by QR.
 - SSR Processing Checklist
 - SSR Cover Letter
 - POC Letter
 - SSR Analysis
- (2) Written responses must be appropriate for forwarding to the agency personnel in response to additional information needed. If any documentation is missing, the quality reviewer must contact the DES/IRS IT Contractor/ITS to load the documentation.
- (3) Verify that the SSR has provided guidance that is complete. There must be a response for every field within the SSR.
- (4) The quality reviewer must review the SSR for grammar, punctuation, spelling and formatting throughout the report. Minor corrections (grammar, punctuation, formatting, etc.) can be made by the quality reviewer without returning/notifying the DES/IRS IT Contractor/ITS. The following items must be reviewed in the SSR.
 1. SSR responses must clearly state current IRS Office of Safeguards policies.
 2. Publication 1075 and NIST references must be cited as appropriate.
 3. Ensure that the agency will fully meet Publication 1075 and NIST standards on the issue if they follow the guidance provided.
 4. Ensure title page references the correct agency.
 5. Outstanding Actions – compare and verify that every item listed is covered in each individual section.
- (5) QR of SSR Transmittal Letter – The quality reviewer must review the transmittal letter that is sent to the agency. The quality reviewer must make minor corrections to the letter. If there are major changes to the letter the quality reviewer must wait until the report is reviewed to load and return the case to the DES/IRS IT Contractor/ITS for re-work.
- (6) Review the transmittal letter for the following:
 1. Verify that correct letter template is used.
 2. Check spelling, grammar, punctuation throughout letter.
 3. Verify that the official is named correctly.
 4. Verify proper title is used in the salutation.
 5. Verify agency name is correct.
 6. Verify the acceptance (or non-acceptance) statement's validity.
 7. Verify correct due dates are referenced.

- (7) QR must take the following actions after reviewing the case:

If ...	Then ...
Case requires minor corrections such as grammatical spelling, grammar, punctuation, spacing and format.	Minor corrections can be made by the Quality Reviewer without returning/notifying the DES/IRS IT Contractor/ITS for rework.

If ...	Then ...
Case requires multiple or major corrections.	<p>Case must be returned to the DES/IRS IT Contractor/ITS for rework.</p> <ul style="list-style-type: none"> • Upload document with recommended changes using the proper naming convention. • Make a case note documenting actions taken and the necessary corrective actions to be taken by DES/IRS IT Contractor/ITS. • Submit case for Rework.
Documentation is missing.	Contact DES/IRS IT Contractor/ITS to upload or input the required documentation.
Case is complete with no required changes.	<ul style="list-style-type: none"> • Follow grading procedures to enter the SSR grade in the eCase title, and include grading information in the processing checklist. • Submit case for Management Approval.

- (8) Update Comments and "Email Notification Comment" under the electronic case management system workspace using the appropriate naming convention format.
- (9) QR must conduct a review of the case within 7 calendar days of SSR case assignment. All Office of Safeguards employees assigned or processing SSRs are required to document in case notes any occurrence resulting in missed timeframes.

11.3.36.11.2
(02-24-2025)
**Quality Review of
Safeguard Review
Reports**

- (1) The S&RT MA must complete the following when a case is assigned to QR:..
 - a. Run and upload to the electronic case management system an open findings report specific to the agency.
 - b. Review the electronic case management system for any open CAP case associated to the previous review for the specific agency and input a case note indicating whether or not there is an open CAP.
- (2) Quality reviewers must utilize the QR SRR Checklist located on the Office of Safeguards SharePoint *Job Resources and Reference Documents* to review the case prior to submitting the case for management approval.
- (3) QR must take the following actions after reviewing the case:

If ...	Then ...
There are open findings listed on the open findings report.	Quality reviewer must email DES and DES' Chief to advise of the open findings and to take the necessary required actions to close the finding(s). Note: If the previous review finding(s) has not been closed by the DES, the report can still move forward.
There is an open CAP case associated with the previous review.	S&RT MA must email S&RT inventory analyst to move CAP case forward, as a new CAP will be generated and sent with the SRR.
Case requires minor corrections such as grammatical spelling, grammar, punctuation, spacing and format.	Minor corrections can be made by the quality reviewer without returning/notifying the DES.
Case requires multiple or major corrections.	Case must be returned to the DES/IRS IT Contractor/ITS for rework. <ul style="list-style-type: none"> • Upload document with recommended changes using the proper naming convention. • Make a case note documenting actions taken and the necessary corrective actions to be taken by DES/IRS IT Contractor/ITS. • Submit case for rework.
Documentation is missing.	Contact DES/IRS IT Contractor/ITS to upload or input the required documentation.
Case is complete with no required changes.	Submit case for Management Approval.

- (4) Update Comments and "Email Notification Comment" under the electronic case management system workspace using the appropriate naming convention format.
- (5) Case must be forwarded for Management Approval within 40 calendar days of receipt. All Office of Safeguards employees assigned or processing SRRs are required to document in case notes any occurrence resulting in missed time-frames.

11.3.36.11.3
(02-24-2025)

**Quality Review of
Technical Inquires**

- (1) QR will be performed on TIs based on the following Issue Code Groups/Issue Codes:

Code Group	Issue Code
A – Record Keeping	A1, A2, A3, A4, A5
B – Secure Storage	B1, B2, B3, B4, B17
C – Restricting Access	C1, C2, C3, C4, C5, C6, C7, C8, C9, C11, C14, C15, C16, C25, C26
D – Other Safeguards	D1, D2, D3, D4
E – Reporting Requirements	E6, E7
G – Need and Use	G1, G2
H – Section H	All

- (2) QR must utilize the QR TI Checklist located on the Office of Safeguards SharePoint *Job Resources and Reference Documents* to review the case prior to submitting the case for management approval.
- (3) For written responses QR must verify the TI Response is formatted correctly. Reference IRM 11.3.36.9.3, TI Processing Procedures.
- (4) QR must take the following actions after reviewing the case:

If ...	Then ...
Issue Code Group/Issue Code is wrong.	Correct Issue Code Group/Issue Code.
Case requires minor corrections such as grammatical spelling, grammar, punctuation, spacing and format.	Minor corrections can be made by the Quality Reviewer without returning/notifying the DES/IRS IT Contractor/ITS for rework.
Case requires multiple or major corrections.	<p>Case must be returned to the DES/IRS IT Contractor/ITS for rework.</p> <ul style="list-style-type: none"> • Upload document with recommended changes using the proper naming convention. • Make a case note documenting actions taken and the necessary corrective actions to be taken by DES/IRS IT Contractor/ITS. • Submit case for rework.

If ...	Then ...
Documentation is missing.	Contact DES/IRS IT Contractor/ ITS to upload or input the required documentation.
Case is complete with no required changes.	Submit case for Management Approval.

- (5) Update Comments and “Email Notification Comment” under the electronic case management system workspace using the appropriate naming convention format.
- (6) TIs must be forwarded by QR for management approval within 25 days of receipt. All Office of Safeguards employees assigned or processing TIs are required to document in case notes any occurrence resulting in missed time-frames.

11.3.36.11.4
(02-24-2025)
**Quality Review of 45
Day Notifications**

- (1) QR will be performed on 45 Day Notifications requiring approval. QR will not review the following 45 Day Notifications:
 - Contractor Acknowledgement Letters
 - Withdrawals
 - Unable to Process Letters
 - Insufficient Information Letters
- (2) ITS will perform QR on any 45 Day Notifications involving the IRS IT Contractor to verify the deliverable:
 - Cloud Computing
 - Live Data Testing
- (3) QR must utilize the QR 45 Day Notification Checklist located on the Office of Safeguards SharePoint *Job Resources and Reference Documents* to review the case prior to submitting the case for management approval.
- (4) In addition to utilizing the QR 45 Day Checklist, QR must review the following in the letter for issuance to the agency:
 - Verify the appropriate notification paragraph(s) have been used.
 - Verify SSR submission method (SDT or email).
 - Verify contact information is correct.
 - Verify AD name and title is correct.
- (5) Verify the Contractor Check Sheet has been completed correctly and reflects that the notification was submitted properly.
- (6) QR must take the following actions after reviewing the case:

If ...	Then ...
Case Sub Type is wrong.	Correct Case Sub Type for the appropriate 45 Day Notification Type.

If ...	Then ...
Case requires minor corrections such as grammatical spelling, grammar, punctuation, spacing and format.	Minor corrections can be made by the Quality Reviewer without returning/notifying the DES/IRS IT Contractor/ITS for rework.
Case requires multiple or major corrections.	Case must be returned to the DES/IRS IT Contractor/ITS for rework. <ul style="list-style-type: none"> • Upload document with recommended changes using the proper naming convention. • Make a case note documenting actions taken and the necessary corrective actions to be taken by DES/IRS IT Contractor/ITS. • Submit case for rework.
Documentation is missing.	Contact DES/IRS IT Contractor/ITS to upload or input the required documentation.
Case is complete with no required changes.	Submit case for Management Approval.

- (7) Update Comments and “Email Notification Comment” under the electronic case management system workspace using the appropriate naming convention format.
- (8) 45 Day Notifications must be forwarded by QR for management approval within 25 calendar days of receipt. All Office of Safeguards employees assigned or processing 45 Day Notifications are required to document in case notes any occurrence resulting in missed timeframes.

11.3.36.12
(02-24-2025)
Safeguard Reviews

- (1) State and Local Agency Safeguard Reviews are conducted by the Safeguard Review Team (SRT) and evaluate an agency’s compliance with the safeguard requirements for the protection of tax returns or return information as prescribed in IRC 6103(p)(4). The level of detail on how the agencies use the data received must be determined to conduct a quality review. The size and diversity of the agency operations makes the determination of the flow of the FTI challenging. The following state agencies receive FTI subject to IRC 6103(p)(4) oversight:
 - State Attorney Generals (AG)
 - Departments of Revenue (DOR)
 - State and Local Child Support (CS) Enforcement Agencies
 - State Human Services (HS) Agencies
 - State Departments of Transportation (DOT)
 - State Workforce Agencies (SWA)
 - Affordable Care Act (ACA)

- (2) Federal Agency Safeguard Reviews are conducted by the Federal Review Team (FRT) and evaluate an agency's compliance with the safeguard requirements for the protection of tax returns or return information as prescribed in IRC 6103(p)(4). Federal Agencies receive data per various statutory code authorizations from various sections of the IRS and Social Security. The level of detail on how the agencies use the data received must be determined to conduct a quality review. The size and diversity of the agency operations makes the determination of the flow of the FTI challenging. Data received is generally different than state agencies and more challenging to identify exact data sets and data elements. Level of detail on both what data they received and what they do with it is generally much less. Size and diversity of agency operations makes identifying the flow of FTI challenging. The following Federal agencies receive FTI subject to IRC 6103(p)(4) oversight:

Federal Agencies	Federal Agencies Continued
Census Bureau	Department of Justice, Federal Bureau of Investigation
Centers for Medicare & Medicaid Services, Center for Consumer Information & Insurance Oversight	Department of Labor
Congressional Budget Office	Department of State
Department of Agriculture	Department of the Treasury, Bureau of the Fiscal Service
Department of Commerce, Bureau of Economic Analysis	Department of Veterans Affairs, Veterans Benefits Administration
Department of Education	Department of Veterans Affairs, Veterans Health Administration
Department of Health & Human Services, Administration for Children and Families, Office of Child Support Services	Office of Personnel Management
Department of Health & Human Services, Departmental Appeals Board	Pension Benefit Guaranty Corporation
Department of Health & Human Services, Office of Medicare Hearings & Appeals	Railroad Retirement Board
Department of Homeland Security, Immigration & Customs Enforcement	Social Security Administration
Department of Homeland Security, Secret Service	U.S. Postal Service

Federal Agencies	Federal Agencies Continued
Department of Justice	Additional Federal agencies enforcing non-criminal or criminal laws which could be included.

11.3.36.12.1
(02-24-2025)
**Safeguard Review
Preparation**

- (1) Federal Agency Pre-review planning
 - a. Seek input from Data Services regarding any Computer Matching Agreements (CMAs) in effect.
 - b. Seek input from the GL if the agency is part of the Federal Intergovernmental Partnering Program or has an IRS point of contact.
 - c. If the agency is using FTI for tax modeling, publishing on the internet, or disclosing for congressional inquiries, invite the Office of SOI to conference calls and ask if they would like to be included in emails to the agency.
 - d. Identify any CMAs, Intergovernmental Partnering Program, Memorandum Agreements, Intergovernmental Partnering Program, Memorandum of Understanding, or Agreements.
- (2) Preparation for all safeguard reviews must be conducted 120 calendar days before the review. Use the following timeframes and actions below to conduct the review preparation. The must be completed as part of the review preparation:

Time Frames	Safeguard Review Preparation
Preparation 90 –120 Calendar Days from the Review	<p>a. Telephone or email the agency point of contact (POC) to introduce yourself, confirm current POC, and review dates.</p> <p>b. Email review contact questionnaire to the POC and set an appropriate deadline (approx. 7 calendar days).</p> <p>Note: If you are unable to determine the primary IRS POC or receive a request for different review dates please contact the Chief, SRT/FRT for assistance.</p> <p>c. Upload completed review contact questionnaire to case using the proper naming convention and update the agency contact information in the case management system.</p> <p>Note: For federal agency reviews, if the scope of the review is large (e.g. US Census), then schedule an initial conference call to discuss steps for the upcoming Safeguard Review.</p> <p>d. Prepare SRR Notification Letter using the address provided by the agency on the Review Contact Questionnaire no later than 60 calendar days from the scheduled review.</p> <p>Note: If the agency does not respond to attempts at contact or complete the Review Contact Questionnaire, then the DES will use information located via internet research, SRR, and the electronic case management system contact information.</p> <p>e. Contact the appropriate GL and Disclosure Manager to inform them of the upcoming agency review, scheduled dates, and determine if there are issues or concerns.</p> <p>f. Research and review agency documents to determine the scope of physical and logical locations for FTI.</p> <ul style="list-style-type: none"> • Determine state or county administration use of FTI. • Determine contractor access to FTI. • Request copies of access lists to FTI and conduct research using the information for the review to determine the scope of the review.

Time Frames	Safeguard Review Preparation
Preparation 60 – 90 Calendar Days from the Review	<p>a. Ensure the agency has the latest copy of Publication 1075, if not refer them to the <i>Office of Safeguards website</i>.</p> <p>b. Provide the following Sample Data Request to each agency type:</p> <ul style="list-style-type: none"> • Sample Agenda • Review Prep Questionnaire (RPQ) • Internal Inspection Templates • Visitor Access Log Sample • Data Tracking Log Sample • Disclosure Awareness Products List <p>c. Schedule conference call(s), discuss documents needed for review, provide the expectations for the agency.</p> <p>d. Set a deadline for the receipt of the above listed documents.</p> <p>e. Prior to the PSE call explain the purpose of the PSE call and the importance of having correct IT staff involved on the call. Discuss the data flow documents and stress the PSE call cannot be conducted without the PSE Form received prior to the call.</p> <p>f. The Office of Safeguards DES and IRS ITS must conduct the PSE call and address any open questions to assist with determining the scope. The PSE call will focus on the following:</p> <ul style="list-style-type: none"> • Number and type of computer platforms operational within the agency. • Data requests for control and requirements. • Verification of evidence. <p>Note: Advise PSE scheduler that a county run office needs a separate PSE call scheduled. Attend PSE calls for county run field offices, contracted collection agencies and contractor/ subcontractor sites that have non agency owned technologies that contain FTI.</p>

Time Frames	Safeguard Review Preparation
Preparation 30 – 60 Calendar Days from the Review	<ul style="list-style-type: none"> a. Schedule a call with the POC to discuss Review Prep Questionnaire (RPQ) in detail. Explain the different sections and the importance of getting the correct information. b. Conduct analysis of SSR, SRR, CAP, RPQ, 45 Day Notifications, TIs taking notes from research conducted. c. Review the agency org chart (if not available in SSR/Internet/provided) d. Remind agency of any final deadlines for documents, data flow, and the RPQ.
Preparation 0 – 30 Calendar Days from the Review	<ul style="list-style-type: none"> a. Follow up with agency for remaining documentation three weeks prior to the on site review. b. DES must coordinate and communicate with the IRS IT Contractor/ITS assigned to the agency. c. Review the agenda with the POC including any dates, times, and addresses for site locations. A copy of the agenda must be provided to the IRS IT Contractor/ITS and Chiefs SRT/FRT. d. Review policies, procedures and the RPQ documenting in the electronic case management system note(s) what was reviewed and note any issues or concerns. e. One week prior to review; print Review Opening Presentation, sign in sheets for opening and closing conference and coordinate with the IRS IT Contractor/ITS assigned to your agency regarding logistics. Provide opening conference date and time to the GL. f. Hold final discussion with the agency POC, make changes to the agenda if needed, ensure the agency will have appropriate IT, policy or business related employees at opening conference. Make sure the opening conference room will have a white board or easel for use and that Office of Safeguards staff will have a room to work from.
Time Frames	ITS/IRS IT Contractor Safeguard Review Preparation
Preparation 60 – 90 Calendar Days from the Review	<ul style="list-style-type: none"> a. Conduct pre-review outreach email to have agency complete PSE document. b. Schedule and conduct PSE Call.

Time Frames	ITS/IRS IT Contractor Safeguard Review Preparation
Preparation 30 – 60 Calendar Days from the Review	<ul style="list-style-type: none"> a. Send out Post-PSE email. b. Conduct any Mini-PSE calls required for contractor or field office locations.
Preparation 0 – 30 Calendar Days from the Review	<ul style="list-style-type: none"> a. Conduct Nessus/IT schedule Prep call. b. Prepare IT Scope Memo. c. Prepare Final Review Schedule.

- (3) Review and analyze the following documents and any other sources that can provide information for the review.

Document	Information for the Review
45 Day Notifications	Review Notifications to identify contractors, subcontractors, tax modeling, live data testing, or cloud computing.
Agency Website	Identify agency structure and other general agency information by researching their internet website. If an organizational chart is available, load this into the case.
CAPs	Documents how prior findings were closed and agency responses to findings which remain open.
Data Services Report	Review report to determine the type and volume of disclosures made to the agency and to the contractor. Review their Transcript Delivery System (TDS) report to determine what transcripts were requested and printed by state agencies.
Publication 1075	Tax Information Security Guidelines for Federal, State and Local Agencies
SDSEM	If previous reviews were conducted, the work papers are examined to determine prior location, departments, and policies which resulted in prior findings.
SRR	If previous reviews were conducted, the reports are examined for previous findings, recommendations, and follow-up actions.
SSR	The SSR must always be reviewed against the subsequent and prior SSRs. The SSRs provide useful information regarding current Responsible Officer(s), the number of offices inspected, latest FTI destroyed, enhancements to computer systems, locations of federal tax information.

Document	Information for the Review
Studies and Audits	GAO and other studies conducted of an agency's general and data processing operation could provide pertinent information.
TIGTA	Treasury Inspector General for Tax Administration (TIGTA) could have information about the agency that could have an impact on the sharing of FTI.
TIs	Document prior and possible outstanding questions from the agency.
Additional Information, as Needed	<p>Documentation by Agency Type</p> <ul style="list-style-type: none"> • DOR or IRC 6103(d) review: Basic Agreements, Implementing Agreements, Governmental Liaison Data Exchange Program (GLDEP) enrollments, GLDEP Need in Use Justification, Memorandum of Understandings (MOUs), agency IRC 6103(p)(2)(B) agreements, and TDS records. • Department of Human Services or IRC 6103(l)(7) review: CMA with SSA for review of BEER. IRS CMA from Data Services and the agency. Income and Eligibility Verification Systems (IEVS) counts from Data Services for previous 3 years. • Child Support Services IRC 6103(l)(6), IRC 6103(l)(8), and IRC 6103(l)(10) • Review Service Level Agreements, 45 day contractor notification letters, and agency contracts.

Note: IRS IT Contractors can be assigned to a SRR for the Computer Security Review preparation, reference IRM 11.3.36.1.3, Roles and Responsibilities for additional information.

- (4) Prior to the review, a preparation call must be conducted and will include the responsible Chief, SRT/FRT, DES, IRS IT Contractors/ITS and appropriate GL representative.
- For State and Local agency Reviews complete the Safeguards Onsite Review Preparation Check List and email the Review Prep Doc located on the Office of Safeguards SharePoint *Job Resources and Reference Documents* to the responsible Chief and MA.
 - For Federal Agency Reviews complete Federal Review Scope Document which must include information from the Onsite Review Preparation Check List and additional information on the Background, Code Authority, all locations where FTI resides, IT Data Flow and Computer Security Scope.
 - Upload the Review Prep Doc no later than one working day prior to the Prep Call using the proper naming convention.
 - DES must work with the IT Contractor/ITS to complete the Computer Security section of the Review Prep Doc.

(5) Travel Coordination

- No more than 30 calendar days prior to the review, the DES must have the travel authorization complete, signed and ready for management approval. This needs to include the airline reservation and car rental. If the DES will be traveling by private vehicle ensure a cost comparison worksheet is included in the authorization.
- Each traveler must fill out the travel itinerary by the required deadline.
- The Lead DES must compile the travel itinerary information into one document and share with all parties prior to the review.

11.3.36.12.2

(02-24-2025)

**Conducting the
Safeguard Review**

(1) The week of the cybersecurity review the CSR must conduct the following in accordance with the schedule:

a. Execute technical SCSEMs

Note: To the greatest extent possible, the CSR must observe (e.g., via screen sharing) and document settings, configurations, and behaviors to verify technical implementation of the SCSEMs.

b. Conduct automated testing by utilizing Nessus Scans.

Note: To the greatest extent possible, automated tests/scan must be observed (e.g., via screen sharing) by the CSR .

c. Conduct interviews and review documentation as appropriate.

d. Provide a summary of the daily accomplishments, risks, issues to the DES and SRT/FRT Chief

Note: IRS IT Contractors can be assigned to a SRR to conduct the Computer Security Review preparation, reference IRM 11.3.36.1.3, Roles and Responsibilities for additional information.

(2) Onsite Safeguard Reviews

- a. DES must communicate with the IRS IT Contractor/ITS regarding travel times and locations for the review if applicable.
- b. The purpose of the opening conference is to acquaint agency officials with plans for the review and to make any adjustments to the necessary arrangements and accommodations for this review.
- c. Review Opening Conferences are generally held at 9:00 am the first day of the review but this is subject to adjustment based on the scope of the review and travel logistics. This decision will be made by and between the Chief, SRT/FRT and the State IRS IT Contractor/ITS Lead.
- d. In general, the walk-through of the data center is scheduled at 11:00 am or 1:00 pm the first day of the review and is attended by all DES who have verified data at the data center. Exceptions will be made on a case by case basis and approved by the Chief, SRT/FRT. A set time must be scheduled for all team members to conduct one review of a State consolidated data center.
- e. Lead DES and Chief, SRT/FRT will work with members of the team to ensure alternate sites are covered during the review.

Example: The DES assigned to DOR might cover an offsite storage facility for the DES assigned to CS.

- f. Advise Chief, SRT/FRT or management of any additional devices that need to be added to the IT scope.

- (3) Onsite Safeguard Review Management Processes for Chief SRT/FRT.
- a. Responsible for all actions occurring during the course of the onsite review and provides oversight for travel coordination issues.

b. Manages the review process onsite by maintaining good communications with team members, and by being available to the agency, if necessary.

c. Conducts daily post review meetings to review the events of the day. Topics must include a review of Critical findings, commonalities between agencies, future items for review the following day, and any other concerns.

d. Provides guidance and oversight to any applicable contractor personnel onsite.

e. Attends at least one opening, schedules all closings, and must be onsite with as many agencies as possible based on logistical constraints.

f. Is the final arbiter for any onsite mitigation proposed by the agency.

g. Is responsible for determining if a review is held as a preliminary closing and must provide oversight for coordinating follow-up activities for preliminary closings.

11.3.36.12.3

(02-24-2025)

Review Techniques

- (1) **Interviews** – The interview method is the process of holding discussions with individuals or groups of individuals within an organization to facilitate assessor understanding, achieve clarification, or obtain evidence. During the review, agency employees, contractors and subcontractors will be interviewed. Interviews are valuable in that they provide information based on personal experience. This information can help determine the extent of disclosure, safeguards and security awareness as well as awareness of penalty provisions of IRC 7213, IRC 7213A, and IRC 7431. Additionally, interviews can provide answers to questions regarding operations and procedures. Interviews do not have to be restricted to employees and can be conducted with third parties (e.g., custodians, security guards, other tenants) to gather information on the measures used to restrict access to areas housing tax data.
- (2) **Examination** – The examine method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities) to facilitate assessor understanding, achieve clarification, or obtain evidence. Observing actual agency onsite operations is a required step in the review process. The DES must tour the areas or departments which handle or store FTI, including the data processing center, regardless of whether it is agency-operated, a shared facility or a contractor facility that receives processes, transmits or stores FTI. The DES must note actual written policy and procedures, actual operational execution of these policies and procedures, as well as work flow. The inspection must also provide information about the following:

Security Measures	Security Measures Continued
Perimeter Security	Emergency procedures, including data breaches and incident management
Containerization	Destruction and disposal
Keys and combination controls	Computer system security (including alternate work sites)

Security Measures	Security Measures Continued
Intrusion alarms	Call and payment centers
Physical access controls	Collection agencies
Storage and handling	Additional contractor and subcontractor physical and logical access when reviewing additional locations.

Note: Address contractor and subcontractor physical and logical access when reviewing additional locations

- (3) **Testing** – The test method is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare the actual state of the object to the desired state or expected behavior of the object.
- (4) **Background Check** – DES must inspect and evaluate agency policy and procedure related to background investigations of employees and contractors with access to and use of FTI as well as a sample of completed employee and contractor background investigations. DES will document on a SRR and CAP the finding and require corrective action by agency of any failure to comply with IRS published standards for agency background investigation requirements. DES will note on a SDSEM any compliance failures associated with specific test cases established with regard to IRS published standards for agency background investigation requirements. SDSEM Test cases to evaluated for compliance include:
- Does the agency have a policy requiring a background investigation of each employee and contractor with access to and use of FTI?
 - Does the policy require the initiation of a background investigation prior to permitting newly hired employees or contractors access to or use of FTI?
 - Does the policy establish an unfavorable background investigation result criterion for each required element which, if found, would result in preventing or removing an employee's or contractor access to and use of FTI?
 - Does the policy require that reinvestigations are initiated for each existing employee and contractor with access to FTI not less than 5 years from the date of their previous background investigation?
 - Does the policy specify that, at minimum, background investigations must include:

Step	Background Investigations
1.	Fingerprinting or review of Federal Bureau of Investigations (FBI) fingerprint results?
2.	Checks at local law enforcement agencies where the subject has lived, worked, and/or attended school within the last 5 years, and if applicable, of the appropriate agency for any identified arrests?

Step	Background Investigations
3.	Citizenship/residency checks to validate the subject's eligibility to legally work in the United States (e.g., a United States citizen or foreign citizen with the necessary authorization).

- f. Does the agency have a procedure that describes the roles, responsibilities and actions required to ensure background investigation policy requirements are timely initiated, completed, and unfavorable results are adjudicated?
- g. Did the agency provided sample of completed employee and contractor background investigations include documentation of:

Background Investigation Documentation	Example
Citizenship/Residency Check	A dated screen print from the E-Verify website or a green card.
Fingerprint Check	FBI fingerprint results of dated certification by a memorandum official that favorable FBI fingerprint results were received.
Local Criminal Check	A dated certification from a local law enforcement agencies regarding the existence or non-existence of any record of criminal activity or dated certification by a management official that favorable local law enforcement criminal check was completed.

- (5) **Case file reviews** – These consist of spot checks of agency files and the examination of records that contain FTI.

11.3.36.12.4
(02-24-2025)

Team Coordination

- (1) Communication between team members, as the review is progressing, is vital and beneficial, as it can identify problems and provides information that alters or expedites the review plan. The DES must communicate shared findings with other DES reviewing other agencies. Ensure shared findings match on all agencies PFRs.
- (2) Set aside time during the closing conference to discuss the findings with POC. This allows the agency the opportunity to hear the findings and start on remediation.
- (3) The PFR and recommendations must be discussed at the closing conference. This allows the agency the opportunity to better understand what the reviewer/team has found and provide additional information, should the agency see the need to do so.
- (4) Critical findings must be reported to the Chief immediately, who will then communicate to the Area Manager.
- (5) IRS IT Contractor/ITS and DES must maintain regular communication during the review.

Example: A potential increase in scope is discovered, the IRS IT Contractor/ITS contacts the DES to identify any other information that impacts the review.

- (6) A deadline must be set with the agency POC for needed policy and procedures not previously provided no later than 2:00 p.m. the day before the closing.

11.3.36.12.5
(02-24-2025)

Need and Use Reviews

- (1) A Need and Use Review of each agency receiving FTI must be conducted as part of the Safeguard Review.
- (2) A Need and Use Review is considered verification or confirmation of the Need and Use Justification made prior to the release of the requested tax information to the state agency
- (3) Compare FTI the agency is using versus FTI received. Determine if the agency should continue to receive all of the FTI. If not, advise the GL and the Disclosure Manager as appropriate. Document the PFR with the appropriate findings.
- (4) Ensure the agency is compliant with IRS statutes, Federal regulations, existing agency agreements (basic and implementing) service policies and MOU's.
- (5) The scope of the review must be broad enough to provide the reviewer with sufficient information to document a conclusion as to the agency's need for and use of FTI.
- (6) Other key areas to be reviewed would include (but are not limited to):
 - a. Routine exchanges
 - b. Joint projects or other specific exchanges
 - c. SLAs and MOUs
- (7) Verify the Need and Use Justification Statement for Use of Federal Tax Information for Tax Modeling, Revenue Estimation or other Statistical Purposes.

Note: Non-use of tax data does not necessarily constitute FTI misuse. However, the objective is to reduce or eliminate unnecessary disclosures of FTI. If the original Need and Use Justification was valid, but the actual utilization has been postponed, the reviewer's responsibility is to evaluate whether there is a reasonable expectation that continued retention of the data will be of value to the state for tax administration within a reasonable and logical timeframe.

11.3.36.12.6
(02-24-2025)

Preliminary Findings Report Preparation

- (1) The PFR identifies the items requiring correction as a result of an IRS Office of Safeguards review. For each finding, the evaluated risk for potential loss, breach or misuse of FTI establishes the recommended timeframe for resolution. The risk category is noted next to each finding in this report to assist the agency in establishing priorities for corrective action. See also IRM 11.3.36.6, Safeguards Preliminary Findings Report for information on preparing the PFR.
- (2) The DES must complete the PFR during the onsite review. The title page, footer and Section E must be complete prior to the review. The document must be completed including the computer security review findings in Section H and submitted to the POC before the closing conference. The standardized findings

with associated risk category are available on the SRR Standardized Findings Language Document located on the Office of Safeguards SharePoint *Job Resources and Reference Documents*.

Note: The DES is responsible for the PFR in its entirety to include Section H. If any corrections need to be made or are identified during the Closing Conference the DES is responsible for incorporating the corrections and uploading the accurate PFR post closing. This includes any Section H corrections.

- (3) SRT/FRT must implement required actions to initiate IRC 6103(p)(7) recommendation prior to issuance of the PFR. Reference IRM 11.3.36.16, Enforcement for additional information.

11.3.36.12.7
(02-24-2025)

Closing Conference

- (1) In general, the closing conference time will be discussed during the first evening meeting with the Chief, SRT/FRT and finalized as soon as possible thereafter.
- (2) Closings must be scheduled according to scope, resources, agency availability and the Office of Safeguards availability with the final time and date signed off by the Chief, SRT/FRT.
- (3) Email the agency POC the time of the closing conference.
- (4) Review the risk categories – emphasizing the Critical and Significant risks. The DES will review findings in sections A - G and the IRS IT Contractor/ITS will review section H. Remind agency personnel that changes in procedures made to comply with recommendations must be documented in the CAP.
- (5) Remind agency when the next SSR and CAP is due. Always ask the agencies if they have any questions before the close of conference

Note: During the closing conference inform the agency that DES is the point of contact until the final report SRR and CAP are issued.

- (6) Advise the agency for any Critical Risk findings, the agency must submit an agency response plan to address the Critical Risk findings within 5 business days of the closing conference. The DES must do the following regarding the agency's response plan:

If ...	Then ...
The agency submits the response plan.	<ul style="list-style-type: none"> a. Email a copy of the plan to the Chief, SRT/FRT and ITS. b. DES must conduct an analysis of any Section A-G Critical Risk findings c. ITS must prepare the Critical Response Analysis for any Section H Critical Risk findings. d. Document receipt in case management system.

If ...	Then ...
There is no response within 5 business days of the Closing Conference.	Follow up with the agency and issue a deadline to receive the a copy of the plan within 2 business days.
There is no response within 2 business days of the second deadline.	Notify the Chief, SRT/FRT the plan has not been filed after two attempts. Chief SRT/FRT will elevate the issue to secure the plan and have a Critical Response Analysis prepared.

Note: IRS IT Contractors can be assigned to provide the Critical Response Analysis, reference IRM 11.3.36.1.3, Roles and Responsibilities for additional information.

11.3.36.12.8
(02-24-2025)
Work Papers

- (1) Review Contact Questionnaire used to secure the name, address, telephone number, and email address for an agency's director/commissioner, an Information Technology (IT) contact, and the primary POC.
- (2) Review Prep Questionnaire used to secure information on the areas within an agency that receive, store, transmit and process FTI from receipt to destruction.
- (3) Agenda with physical locations and contact numbers
- (4) SDSEM used to note any compliance failures, with regard to IRS published standards, identified through the use of review techniques.
- (5) Critical Mitigation Plan used to identify how Critical findings from the review will be addressed, if applicable.

Note: Work papers from the review must be uploaded to the case, as an attachment, in the case management system.

11.3.36.13
(02-24-2025)
Inventory and Management Reports

- (1) Inventory management is critical to effective safeguarding of FTI.
- (2) Inventory Management occurs on a daily basis, and is to be reported out to the AD at the minimum of once per week.
- (3) Chiefs, SRT/FRT, Analysts, TAs, and IRS IT Contractor support are required to work in concert to give the AD the most accurate snapshot of inventory status possible. This will include reporting out on current status of the following items:
 - TIs
 - 45 Day Notifications
 - SRRs
 - SSRs
 - CAPs

- | | |
|---|---|
| 11.3.36.13.1
(02-24-2025)
Technical Inquires and Notifications | (1) The Technical Inquiry & 45 Day Notification weekly inventory report is based on an electronic case management system query that focuses on the case types of TIs and 45 Day Notifications. All statuses EXCEPT "Release" are included in the query. TIs and 45 Day Notifications have a due date of 30 calendar days from receipt of inquiry . |
| 11.3.36.13.2
(02-24-2025)
Safeguards Review Report | (1) The SRR weekly reporting is based on an electronic case management system query that focuses on "DES assignment" and "due date". All states EXCEPT "Release" and Intake are included in the query. SRRs have a 45 calendar day completion date with a start time based on the closing conference date of the review.

(2) The S&RT Analyst must produce a weekly SRR inventory report. The SRR will be shared with the Chiefs, SRT/FRT on a weekly basis (or as required by Chiefs, SRT/FRT) to maintain workload accountability and inventory control. The query will be produced in Excel format unless otherwise determined by Chiefs SRT/FRT. |
| 11.3.36.13.3
(02-24-2025)
Safeguards Security Report | (1) The SSR weekly reporting is based on "IRS contractor assignment" and "due date". All processing status EXCEPT "Release", "Intake", and Awaiting Agency Response are included in the query. SSR's have a 60 calendar day completion date with a start time based on the date the SSR was received in the Safeguards mailbox.

(2) The S&RT Analyst must produce a weekly SSR inventory report. The SSR will be shared with the AD, TAs, and Chiefs, SRT/FRT on a weekly basis (or as required by Chiefs, SRT/FRT) to identify any areas of concern and to ensure timely processing of reports in compliance with contractual guidance, maintain workload accountability and inventory control. IRS ITS Contractor will be assigned as "Case Responsible" for all SSR cases. The query will be produced in Excel format unless otherwise determined by AD, TAs and/or Chiefs, SRT/FRT . |
| 11.3.36.13.4
(02-24-2025)
Corrective Action Plan | (1) The CAP weekly reporting is based on an electronic case management system query that focuses on agencies where open findings exist on the Plan of Actions and Milestones (POA&M). This indicates that the findings need to be addressed in a CAP. The report focuses on DES assignment, IRS IT Contractor/ITS assignment and due date. All processing status except Release, Intake and Awaiting Agency Response are included in the query. CAPs have a 45 calendar day completion date with a start time based on the date the CAP was received in the Office of Safeguards Mailbox.

(2) The S&RT Analyst must produce a weekly CAP inventory report. This report will be shared with AD, TAs, and Chief's SRT/FRT on a weekly basis (or as required by Chiefs, SRT/FRT) to identify any areas of concern and to ensure timely processing of reports in compliance with contractual guidance, maintain workload accountability and inventory control. DES will be assigned on an alternating basis as Case Owner , with subordinate assignments to DES staff (for Sections A - G), and to the IRS IT Contractor/ITS (for Section H) for all CAP cases. IRS IT Contractor/ITS will be responsible for assisting with working Section H of the CAPs on an as needed basis as determined by the Chiefs, SRT/FRT. The IRS IT Contractor will be responsible for reporting the status of |

active CAP's during weekly inventory call (see note below). The query will be produced in Excel format unless otherwise determined by AD, TAs, and/or Chiefs, SRT/FRT.

11.3.36.14
(02-24-2025)
**Management Information
Reports**

- (1) In order to assist in monitoring and assessing the Safeguard Review Program, and to provide input for Reports to Congress see also IRM 11.3.36.15, Report to Congress the PA will submit statistical reports to the AD, Office of Safeguards, as required, for tracking purposes. In addition, all DES actions will be reflected in the electronic case management system history.
- (2) Accurate program tracking requires that all data maintained reflect all agencies subject to safeguards, and accurate recording of reviews scheduled, in process, and completed.

Reminder: This data will be cross-checked with the data reflected in the electronic case management system database.

- (3) SSR submission and acceptance, and Need and Use Reviews are also tracked in an effort to ensure agency and contractor compliance with program requirements.
- (4) Occasionally, empirical reports are requested in conjunction with narrative reports describing program accomplishments and shortcomings to establish program goals or guidance for subsequent program emphasis.

11.3.36.15
(02-24-2025)
Report to Congress

- (1) An annual report to Congress regarding the procedures and safeguards of recipients is prepared by the Office of Safeguards.
- (2) The responsible analyst/specialist, in the Office of Safeguards, will submit the report on or before March 31 to the AD, Office of Safeguards. The report is channeled through appropriate management levels for the Commissioner's signature.
- (3) The report will be based on information entered into the electronic case management system database and other safeguards activity throughout the calendar year, e.g., workshops such as Federation of Tax Administrators, speaking engagements at external agencies, serving on IRS implementation teams for new legislation, review/commenting on agreements (e.g., CMAs, IAGs, MOUs), etc. All information for Safeguard Review is to be entered by December 31. The information on safeguard review findings is based on the final Safeguard Review Reports.

11.3.36.16
(02-24-2025)
Enforcement

- (1) IRC 6103(p)(4) provides that IRS must take such actions as are necessary to ensure that the safeguard requirements are being met. Such actions can include refusing to disclose returns or return information until it is determined that the requirements have been or will be met.
- (2) Safeguards Staff must reference IRM 11.3.36.4, Documentation and IRM 11.3.36.1.7, Related Resources for additional information on enforcement and documenting enforcement actions.

11.3.36.16.1
(02-24-2025)

**Guidelines for
Safeguards Task
Alliance Team (STAT)
Enforcement of
Safeguard Reporting
Requirements**

- (1) Follow required actions below when SSRs have not been filed for two consecutive reporting years as follows:

Step	No filing for first reporting year after:
a.	STAT team has received no response within 2 business days after calling POC regarding late SSR
b.	STAT team has received no response within 2 business days to follow-up email advising POC of late SSR
c.	AD has sent STAT prepared letter to advise HOA of efforts to secure late SSR and advised of next SSR deadline
d.	Automatic/granted extension(s) (must not exceed a total of 60 days) deadlines have passed, and AD has sent STAT prepared letter to advise HOA of efforts to secure late SSR and advised of next SSR deadline

Step	No filing for successive reporting year when:
a.	Filing deadline has passed no extension permitted
b.	AD has sent STAT prepared letter to remind HOA of the previous year's non-filing and warning that guidelines have been met to initiate IRC 6103(p)(7) Warning Letter
c.	No filing is received within six months of filing deadline

- (2) Follow required actions below when CAP have not been filed for two consecutive reporting periods as follows:

Step	No filing for first reporting period after:
a.	STAT team has attempted call to POC regarding late SSR
b.	STAT team has sent follow-up email to advise POC of late SRR
c.	AD has sent STAT prepared letter to advise HOA of efforts to secure late CAP and advised of next CAP deadline
d.	Automatic extension (must not exceed a total of 30 days) deadline has passed, and AD has sent STAT prepared letter to advise HOA of efforts to secure late CAP and advised of next CAP deadline.

Step	No filing successive reporting period when:
a.	Filing deadline has passed no extension permitted
b.	AD has sent STAT prepared letter to remind HOA of previous periods non-filing and warning guidelines have been met to initiate IRC 6103(p)(7) recommendation
c.	No filing received within two months of filing deadline

Step	STAT required actions to initiate IRC 6103(p)(7) recommendation:
a.	Ensure that all action regarding attempts to secure successive instances of reporting non-compliance are well documented in eCase
b.	Complete IRC 6103(p)(7) recommendation for FTI suspension and/or termination of FTI Disclosures form
c.	Prepare GLDS Director letter of HOA advising of IRC 6103(p)(7) determination and intent to terminate FTI disclosures and appeal rights
d.	Submit IRC 6103 (p)(7)Recommendation for FTI Suspension and/or Termination of FTI Disclosure from AD for approval along with ARS and STAT prepared GLDS Director letter to HOA advising of IRC 6103(p)(7)determination and intent to terminate FTI disclosures and agency's appeal rights.

11.3.36.16.2
(02-24-2025)

Guidelines for Safeguard Review Team (SRT) Enforcement of Safeguard Requirements Other Than Reporting

- (1) Initiate enforcement recommendation if agency continues to make unauthorized FTI accesses/disclosures.
- (2) Initiate enforcement recommendation if agency will not allow the Office of Safeguards to conduct required reviews, or will not allow the use of automated tools to evaluate security configurations of IT devices.
- (3) Initiate enforcement recommendation if agency does not mitigate findings categorized as Critical Risk (repeat Critical findings).
- (4) Initiate enforcement recommendation if agency has Severe Critical Risk or Multiple Critical Risk findings identified.
 - Severe Critical Risk is determined to have a risk that would preclude the adequate protection of FTI on an enterprise-wide scale.
 - Multiple Critical Risk Is determined to have a volume of Critical findings that would preclude the adequate protection of FTI.

11.3.36.16.3
(02-24-2025)

Enforcement Actions of Safeguard Requirements Other Than Reporting

- (1) In all cases where serious deficiencies are found or where required reports are not submitted, the responsible reviewer will attempt to obtain voluntary compliance through discussion and negotiation.
- (2) When an impasse occurs, involving recipients subject to IRC 6103(p)(4) , the matter must be elevated to the appropriate GLDS management level.
- (3) Communicate with S&RT Chief and ETA to validate the clear requirement for enforcement and document discussion in eCase.
- (4) Required actions to initiate IRC 6103(p)(7)recommendation include:
 - a. DES or ITS (as applicable) provides detailed paragraph to S&RT Analyst describing the reason for enforcement actions and a separate detailed paragraph detailing the required remediation. The ETA will review the paragraph prior to submission to the S&RT Analyst if necessary.

- b. S&RT Analyst prepares and initiates (p)(7) Warning letter for AD approval.
- c. SRT/FRT Chief, DES, and IRS IT Contractor/ITS as applicable, conducts discussion with HOA and applicable agency staff to discuss (p)(7) process and issuance. They also provide agency specific deadline for DES receipt of agency response plan to be shared with TIGTA by SRT/ FRT Chief (7 Days from closing unless otherwise agreed upon). DES must document discussion in SRR case in the case.

11.3.36.16.4
(02-24-2025)
**Associate Director's
Actions**

- (1) If the appropriate management is unable to break the impasse, the recipient agency must be notified in writing of the IRS's preliminary determination and intention to recommend discontinuance of disclosures through the issuance of the (p)(7) Warning Letter.
- (2) Such notices must allow 30 calendar days for response. Notices must indicate:
 - a. That a report is being submitted to the Office of Governmental Liaison Disclosure and Safeguards (GLDS) detailing the uncorrected deficiencies and the agency's reasons, if any, for noncompliance;
 - b. That the Director, GLDS will take appropriate action.

Reminder: The notification must include the appeal and administrative review procedures provided for in 26 CFR 301.6103(p)(7)-1

- (3) At this time, a written report must be prepared and submitted by the AD, Office of Safeguards to the Director, GLDS. The FTI Suspension and/or Termination Memo must follow the following format:

Format	Content
Agency Information	1. Agency Name: 2. Agency Code: 3. Agency Type 4. Head of Agency Name: 5. Head of Agency Phone: 6. Head of Agency Email: 7. Head of Agency Address:
Government Liaison Information	1. Governmental Liaison Name: 2. Governmental Liaison Phone: 3. Governmental Liaison Email Note: Applicable for Federal and Tax Administration Agencies
Disclosure Information	1. Disclosure Manager Name: 2. Disclosure Manager Phone: 3. Disclosure Manager Email

Format	Content
Disclosure Authority and FTI Received	<p>Identify the following:</p> <ol style="list-style-type: none"> 1. Statutory FTI Disclosure Authority 2. Type of FIT Received Electronic? (Yes/No) <ul style="list-style-type: none"> • From what federal or state agency? • Know volume? • Using what connection? 3. Paper? (Yes/No) <ul style="list-style-type: none"> • From what federal or state agency? • Known volume?
IRC 6103(p)(7) Violation(s)	<p>Identified IRC 6103(p)(7) Violations(s)?</p> <ol style="list-style-type: none"> 1. Unauthorized inspection or disclosure of returns or return information and no adequate corrective action taken to prevent recurrence of an unauthorized inspection or disclosure (Yes/No)? If Yes, provide details (What is the violation? How was agency put on notice of violation? How was agency advised to take corrective action? How did agency respond? and/or 2. Section 6103(p)(4) safeguards are not being satisfactorily maintained and agency has demonstrated no adequate plan to improve its system to maintain the safeguards satisfactorily? (Yes/No) If Yes, provide details. (What is the violation? How was agency put on notice of the violation? How was agency advised to take corrective action? How did agency respond?)
Recommendation	<p>Recommend Suspension of FIT Disclosure Pending Final Determination By Commissioner? (Yes/No)</p> <p>Note: If Yes, provide details. (Describe how tax administration would be seriously impaired if FTI disclosures were not suspended pending final determination by Commissioner.</p>
AD Approval	<ol style="list-style-type: none"> 1. AD Approval of IRC 6103(p)(7) Recommendation? (Yes/No) 2. Signature and Date 3. Date Associate Director sent STAT/SRT prepared letter to Head of Agency warning guidelines have been met to initiate recommendation:-

Format	Content
GLDS Approval	<ol style="list-style-type: none"> 1. GLDS Director Approval of IRC 6103(p)(7) Recommendation?(YES/NO) 2. Signature and Date 3. Date GLDS Director sent STAT/SRT prepared letter to HOA advising of IRC 6103(p)(7) determination of intent to terminate FTI disclosures and providing agency appeals rights:
Notification of Appeal Rights from Commissioner's Office to Agency	<ol style="list-style-type: none"> 1. Date Commissioner's Office Notified of Agency IRC 6103(p)(7) Determination Notification: 2. 30 Day Deadline Date for Agency Appeal of IRC 6103(p)(7) Determination: 3. Agency Appealed IRC 6103(p)(7) Determination (Yes/No) <p>Note: If No, Date of Termination of Termination FTI Disclosures to Agency. If Yes, 45 Day Deadline to Commissioner Appeal Conference.</p>
Commissioner Approval	<ol style="list-style-type: none"> 1. Commissioner Sustains IRC 6103(p)(7) Determination (Yes/No)IRC 6103(p)(7). 2. Signature and Date. <p>Note: If Yes, Date of Termination of FTI Disclosures to Agency.</p>

(4) If it is determined that Federal tax administration would be impaired because of a safeguards deficiency, a duly delegated IRS official (see Delegation Order 11-2) can immediately suspend disclosures to the agency pursuant to IRC 6103(p)(4) and 26 CFR 301.6103(p)(7)-1. This would be the case where unauthorized accesses/disclosures would be made absent the suspension. See IRM 11.3.36.16.

(5) If the 30 day time frame expires without the agency taking satisfactory action, a letter must be drafted to the head of the agency from the Delegation Order 11-2 official notifying the agency that disclosures are being discontinued until such time as the deficiency is corrected. Copies of the letter must be sent to the AD, Office of Safeguards and to the Director, Office of GLDS. Documentation detailing the uncorrected deficiencies and the agency's reasons, if any, for noncompliance will be organized and maintained.

Note: There must be appropriate coordination with the Deputy Commissioner's and/or Commissioner's offices from this point forward.

(6) The Director, GLDS actions will be similar to those stated in item 5 above. If the Director is unable to break the impasse, the HOA will be notified in writing of the IRS's preliminary determination and the Director's intention to recommend discontinuance of disclosure. The notice will allow 30 calendar days for response.

- (7) If the 30 day time frame expires without the agency taking satisfactory action, two copies of the proposed letter to discontinue disclosures will be drafted to the HOA, from the Director, Office of GLDS ,notifying the agency that disclosures are being discontinued until such time as the deficiency is corrected. Following the Director's signature, one signed copy will be retained in Headquarters Office, and the other will be forwarded to the AD, Office of Safeguards and to the Director, Governmental Liaison, Disclosure and Safeguards.

11.3.36.16.5
(02-24-2025)

Alternative Actions

- (1) The discontinuance of disclosures can take several forms. The appropriate form is dependent upon all of the facts in the case.
- (2) All disclosures to an agency can be suspended or permanently cutoff in situations where the deficiency pervades the entire agency or where the agency refuses to submit the required reports.
- (3) Suspensions or cutoffs of selected information can be used in cases where the deficiency can be isolated in a certain segment of the agency.

Example: If the deficiency relates to computer processing, electronic disclosures can be suspended while disclosures of paper documents continue.

